

(51) Int.Cl. <sup>7</sup>	識別記号	F I	ページコード <sup>7</sup> (参考)
H 0 4 H	1/02 1/00	H 0 4 H	1/02 1/00
			F 5 C 0 6 4
			B
			F
			H
H 0 4 N	7/16	H 0 4 N	7/16
			Z
審査請求 未請求 請求項の数13 O L (全 16 頁) 最終頁に続く			

(21) 出願番号 特願2001-42624(P2001-42624)

(22) 出願日 平成13年2月20日 (2001.2.20)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 香月 聡一郎

大阪府門真市大字門真1006番地 松下電器

産業株式会社内

(74) 代理人 100081813

弁理士 早瀬 肇一

Fターム(参考) 5C064 BA01 BB02 BC17 BC18 BC22

BC23 BC27 BD02 BD08 CA14

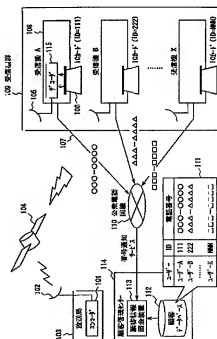
CB01 CC04 DA12

## (54) 【発明の名称】 有料放送システム

## (57) 【要約】

【課題】 I Cカードを使用する有料放送システムにおいて、偽造あるいはコピーされたI Cカードによる不正視聴を発見する。

【解決手段】 顧客管理センター114では、放送局103と有料放送データの視聴契約を締結した各顧客の、氏名、住所、I Cカード106のID番号、受信機108に接続されている公衆電話回線110の電話番号等の顧客情報を、視聴契約時に顧客データベース112にて記録管理し、顧客が前記有料放送データを視聴する場合あるいは視聴した場合、視聴要求あるいは視聴結果とともに受信したID番号及び番号通知サービスの利用により通知された電話番号と、顧客データベース112に記憶されている顧客情報111と、を顧客情報照会装置113にて照合し、照合の結果、番号通知サービスの利用により通知された電話番号と顧客データベース112に記憶されている電話番号とが異なる場合、偽造あるいはコピーしたI Cカード106が使用された可能性があることを判断するようにした。



## 【特許請求の範囲】

【請求項1】有料放送データを提供する放送局と視聴契約を締結した顧客が、該有料放送データを受信可能な受信機を設置して該有料放送データを視聴する有料放送システムにおいて、

有料放送データをエンコードして、スクランブルするエンコーダと、前記スクランブルされた有料放送データを送信する送信アンテナと、を具備する放送局と、

前記放送局から通信衛星を介して前記スクランブルされた有料放送データを受信する受信アンテナと、前記受信アンテナにて受信した前記スクランブルされた有料放送データに対してデスクランブル処理を施し、デコードするデコーダと、前記デスクランブル処理に必要な制御情報及び前記顧客を特定するためのID番号を記憶しているICカードと、公衆電話回線に接続可能なモデムと、を具備する受信機と、

有料放送データの視聴契約時に、氏名、住所、ICカードのID番号、受信機に接続されている公衆電話回線の電話番号等の各顧客に関する顧客情報を記録管理する顧客データベースと、前記顧客情報を必要に応じて照会する顧客照会装置と、を具備する顧客管理センターと、で構成され、

前記顧客が前記有料放送データを視聴する場合あるいは視聴した場合、該顧客が所有する受信機は、番号通知サービスを利用して、前記顧客管理センターへ発呼し前記公衆電話回線を介して行い、視聴要求あるいは視聴結果とともに前記顧客のICカードに記憶されているID番号を前記顧客管理センターへ送信し、前記顧客管理センターは、前記受信したID番号及び前記番号通知サービスの利用により通知された電話番号と、前記顧客データベースに記憶されている前記顧客のID番号及び前記顧客が所有する受信機に接続されている公衆電話回線の電話番号と、を前記顧客情報照会装置にて照会し、前記照会の結果、前記顧客データベースに記憶されている前記顧客が所有する受信機に接続されている前記公衆電話回線の電話番号と前記番号通知サービスの利用により通知された電話番号とが異なる場合、偽造あるいはコピーしたICカードが使用された可能性があると判断する、ことを特徴とする有料放送システム。

【請求項2】請求項1に記載の有料放送システムにおいて、

前記顧客管理センターは、前記顧客データベースに記憶されていない電話番号が通知された場合、あるいは、顧客データベースに記憶されていないID番号が送信された場合、偽造あるいはコピーしたICカードが使用された可能性があると判断する、

ことを特徴とする有料放送システム。

【請求項3】請求項1または請求項2に記載の有料放送システムにおいて、

前記顧客管理センターは、前記偽造あるいはコピーした

ICカードが使用された可能性があると判断した場合、不正視聴した受信機の場所を、前記番号通知サービスの利用により通知された電話番号に基づいて探索する、ことを特徴とする有料放送システム。

【請求項4】請求項1ないし請求項3のいずれかに記載の有料放送システムにおいて、前記ICカードは読み出し専用で、該ICカードに記憶されているID番号は全ての顧客に対して固有のデータである、

ことを特徴とする有料放送システム。

【請求項5】請求項1ないし請求項4のいずれかに記載の有料放送システムにおいて、前記ID番号として、前記ICカードの製造番号を使用する、

ことを特徴とする有料放送システム。

【請求項6】有料放送データを提供する放送局と視聴契約を締結した顧客が、該有料放送データを受信可能な受信機を設置して該有料放送データを視聴する有料放送システムにおいて、

有料放送データをエンコードするエンコーダと、前記エンコードされた有料放送データをスクランブル鍵によりスクランブルするスクランブラと、前記スクランブル鍵を発生するスクランブル鍵発生装置と、マスター鍵により前記スクランブル鍵を暗号化する暗号化装置と、前記暗号化されたスクランブル鍵と前記スクランブルされた有料放送データとを多重化する多重化装置と、前記多重化された有料放送データを送信する送信アンテナと、を具備する放送局と、

前記放送局から通信衛星を介して前記多重化された有料放送データを受信する受信アンテナと、前記多重化された有料放送データに対して復調処理を施すチューナと、前記復調された有料放送データから前記暗号化されたスクランブル鍵及び前記スクランブルされた有料放送データを抽出し、前記スクランブルされた有料放送データに対してデスクランブル処理を施すデスクランブラ・デマルチプレクサと、前記デスクランブルされた有料放送データをデコードするデコーダと、前記放送局にて前記スクランブル鍵の暗号化処理に使用した前記マスター鍵と同一の情報を持つマスター鍵を有し、該マスター鍵を用いて前記デスクランブラ・デマルチプレクサにて抽出された前記暗号化されたスクランブル鍵に対して暗号化復号処理を施し、前記デスクランブル処理に必要なスクランブル鍵として前記デスクランブラ・デマルチプレクサへ出力するICカードと、公衆電話回線に接続可能なモデムと、を具備する受信機と、

有料放送データの視聴契約時に、氏名、住所、ICカードに記憶されているマスター鍵情報、受信機に接続されている公衆電話回線の電話番号等の各顧客に関する顧客情報を記録管理し、前記マスター鍵情報を暗号化装置へ出力する顧客データベースと、前記顧客情報を必要に応じて照会する顧客照会装置と、を具備する顧客管理セン

ターと、  
て構成され、  
前記顧客が前記有料放送データを視聴する場合あるいは視聴した場合、該顧客が所有する受信機は、番号通知サービスを利用して、前記顧客管理センターへ発呼を前記公衆電話回線を介して行い、視聴要求あるいは視聴結果とともに前記顧客のＩＣカードに記憶されているマスター鍵情報を送信し、前記顧客管理センターは、前記ＩＣカードに記憶されているマスター鍵情報及び前記番号通知サービスの利用により通知された電話番号と、前記顧客データベースに記憶されている前記顧客のマスター鍵情報及び前記顧客が所有する受信機に接続されている公衆電話回線の電話番号と、を前記顧客情報照会装置にて照合し、前記照合の結果、前記顧客データベースに記憶されている前記顧客が所有する受信機に接続されている前記公衆電話回線の電話番号と前記番号通知サービスにより通知された電話番号とが異なる場合、偽造あるいはコピーしたＩＣカードが使用されたと可能性があると判断する、  
ことを特徴とする有料放送システム。

【請求項７】請求項６に記載の有料放送システムにおいて、

前記顧客管理センターは、前記顧客データベースに記憶されていない電話番号が通知された場合、あるいは、顧客データベースに記憶されていないマスター鍵情報が送信された場合、偽造あるいはコピーしたＩＣカードが使用されたと可能性があると判断する、  
ことを特徴とする有料放送システム。

【請求項８】請求項６または請求項７に記載の有料放送システムにおいて、

前記顧客管理センターは、前記偽造あるいはコピーしたＩＣカードが使用されたと可能性があると判断した場合、不正視聴した受信機の場所を、前記番号通知サービスの利用により通知された電話番号に基づいて探索する、  
ことを特徴とする有料放送システム。

【請求項９】請求項６ないし請求項８のいずれかに記載の有料放送システムにおいて、

前記ＩＣカードに記憶されている前記マスター鍵情報は、読出し専用で、かつ、全ての顧客に対して固有のデータである、  
ことを特徴とする有料放送システム。

【請求項１０】有料放送データを提供する放送局と視聴契約を締結した顧客が、該有料放送データを受信可能な受信機を設置して該有料放送データを視聴する有料放送システムにおいて、

有料放送データをエンコードするエンコーダと、前記エンコードされた有料放送データをスクランブル鍵によりスクランブルするスクランブラと、前記スクランブル鍵とワーク鍵とを発生するスクランブル鍵発生装置と、前記スクランブル鍵を前記ワーク鍵により暗号化し、さら

に、マスター鍵により前記ワーク鍵を暗号化する暗号化装置と、前記暗号化されたスクランブル鍵と前記暗号化されたワーク鍵と前記スクランブルされた有料放送データとを多重化する多重化装置と、前記多重化された有料放送データを送信する送信アンテナと、を具備する放送局と、

前記放送局から通信衛星を介して前記多重化された有料放送データを受信する受信アンテナと、前記受信アンテナにて受信した前記多重化された有料放送データに対して復調処理を施すチューナと、前記復調された有料放送データから前記暗号化されたスクランブル鍵と前記暗号化されたワーク鍵と前記スクランブルされた有料放送データとを抽出し、前記スクランブルされた有料放送データに対してデスクランブル処理を施すデスクランブラ・デマルチプレクサと、前記デスクランブルされた有料放送データをデコードするデコーダと、前記放送局にて前記ワーク鍵の暗号化に使用した前記マスター鍵と同一の情報を持つマスター鍵を有し、該マスター鍵を用いて前記デスクランブラ・デマルチプレクサにて抽出された前記暗号化されたワーク鍵に対して暗号化復号処理を施し、該復号化されたワーク鍵を記憶し、さらに、該ワーク鍵を用いて前記暗号化されたスクランブル鍵に対して暗号化復号処理を施し、前記デスクランブル処理に必要なスクランブル鍵として前記デスクランブラ・デマルチプレクサへ出力するＩＣカードと、公衆電話回線に接続可能なモジュールと、を具備する受信機と、  
有料放送データの視聴契約時に、氏名、住所、ＩＣカードに記憶されているマスター鍵情報、該マスター鍵により暗号化あるいは暗号化復号処理されたワーク鍵情報、受信機に接続されている公衆電話回線の電話番号等の各顧客に関する顧客情報を記録管理し、前記スクランブル鍵発生装置にて発生した前記ワーク鍵を暗号化するための前記マスター鍵を暗号化装置へ出力する顧客データベースと、前記顧客情報を必要に応じて照会する顧客照会装置と、を具備する顧客管理センターと、  
で構成され、

前記顧客が前記有料放送データの視聴する場合あるいは視聴した場合、該顧客が所有する受信機は、番号通知サービスを利用して、前記顧客管理センターへ発呼を前記公衆電話回線を介して行い、前記視聴要求あるいは前記視聴結果とともに前記ＩＣカードに記憶されたワーク鍵情報を前記顧客管理センターへ送信し、前記顧客管理センターは、前記送信されたワーク鍵情報及び前記番号通知サービスにより通知された電話番号と、前記顧客データベースに記憶されている前記顧客のワーク鍵情報及び前記顧客が所有する受信機に接続されている公衆電話回線の電話番号と、を前記顧客情報照会装置にて照合し、前記照合の結果、前記顧客データベースに記憶されている前記顧客が所有する受信機に接続されている前記公衆電話回線の電話番号と前記番号通知サービスの利用によ

り通知された電話番号とが異なる場合、偽造あるいはコピーしたＩＣカードが使用された可能性があると判断する。

ことを特徴とする有料放送システム。

【請求項１１】請求項１０に記載の有料放送システムにおいて、

前記顧客管理センターは、前記顧客データベースに記憶されていない電話番号が通知された場合、あるいは、顧客データベースに記憶されていないワーク鍵情報が送信された場合、偽造あるいはコピーしたＩＣカードが使用された可能性があると判断する。

ことを特徴とする有料放送システム。

【請求項１２】請求項１０または請求項１１に記載の有料放送システムにおいて、

前記顧客管理センターは、前記偽造あるいはコピーしたＩＣカードが使用された可能性があると判断した場合、不正視聴した受信機の場所を、前記番号通知サービスの利用により通知された電話番号に基づいて探索する、ことを特徴とする有料放送システム。

【請求項１３】請求項１０ないし請求項１２のいずれかに記載の有料放送システムにおいて、前記ＩＣカードに記憶される前記ワーク鍵情報は、更新可能である。

ことを特徴とする有料放送システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、伝走路に衛星波や地上波を用いた有料放送システムに関するものである。

【０００２】

【従来の技術】現在、世界中で衛星波や地上波によるデジタルテレビ放送サービスが行われている。有料放送では、CAS (Conditional Access System) と呼ばれる、視聴契約を締結した顧客だけが番組を視聴でき、それ以外の人には視聴できないようにする技術システムが導入されている。

【０００３】CASには、信号を操作し放送内容からなくなるスクランブル技術とスクランブルを解くための鍵を暗号化して送信する技術が利用される。スクランブル処理を行うスクランブラは操作の方法を随時変えて不正行為が発生しないようにし、スクランブルを解除するデスクランブラは、スクランブルをかけるときに使った鍵を使って解除する。鍵は番組と一緒に放送波で送信されるが、鍵をそのまま送信すると不正行為が起こりやすくなるため、鍵は暗号化して送信される。鍵は、送信側でさらに別の鍵（マスタ鍵）を使って暗号化され、このマスタ鍵は、契約した視聴者に提供されるＩＣカードに記憶される。

【０００４】デジタルテレビ放送のCASにおいて、一般にＩＣカードが使用されている理由は、偽造あるいはコピーしたＩＣカードが出回った場合、不正行為が行わ

れる前に使用していたＩＣカードを使用不可能にし、新たなＩＣカードを各顧客に再発行することで、不正視聴に対する被害を食い止めることができるようにするためである。

【０００５】

【発明が解決しようとする課題】しかし、ＩＣカードの数は、視聴契約した顧客の数だけ存在するため、偽造あるいはコピーしたＩＣカードが出回った場合に再発行されるＩＣカードの数もそれだけ大量になる。

【０００６】本発明は、上記問題を解消するためになされたものであり、不正視聴が行われていないかどうかを随時チェックする機能を有する有料放送システムを提供するものである。

【０００７】

【課題を解決するための手段】上記課題を解決するために、本発明の請求項１に係る有料放送システムは、有料放送データを提供する放送局と視聴契約を締結した顧客が、該有料放送データを受信可能な受信機を設置して該有料放送データを受信する有料放送システムにおいて、有料放送データをエンコードして、スクランブルするエンコーダと、前記スクランブルされた有料放送データを送信する送信アンテナと、を具備する放送局と、前記放送局から通信衛星を介して前記スクランブルされた有料放送データを受信する受信アンテナと、前記受信アンテナにて受信した前記スクランブルされた有料放送データに対してデスクランブル処理を施し、デコードするデコーダと、前記デスクランブル処理に必要な制御情報及び前記顧客を特定するためのＩＤ番号を記憶しているＩＣカードと、公衆電話回線に接続可能なモデムと、を具備する受信機と、有料放送データの視聴契約時に、氏名、住所、ＩＣカードのＩＤ番号、受信機に接続されている公衆電話回線の電話番号等の各顧客に関する顧客情報を記録管理する顧客データベースと、前記顧客情報を必要に応じて照会する顧客照会装置と、を具備する顧客管理センターと、で構成され、前記顧客が前記有料放送データを視聴する場合あるいは視聴した場合、該顧客が所有する受信機は、番号通知サービスを利用して、前記顧客管理センターへ発呼を前記公衆電話回線を介して行い、視聴要求あるいは視聴結果とともに前記顧客のＩＣカードに記憶されているＩＤ番号を前記顧客管理センターへ送信し、前記顧客管理センターは、前記受信したＩＤ番号及び前記番号通知サービスの利用により通知された電話番号と、前記顧客データベースに記憶されている前記顧客のＩＤ番号及び前記顧客が所有する受信機に接続されている公衆電話回線の電話番号と、を前記顧客情報照会装置にて照会し、前記照会の結果、前記顧客データベースに記憶されている前記顧客が所有する受信機に接続されている前記公衆電話回線の電話番号と前記番号通知サービスの利用により通知された電話番号とが異なる場合、偽造あるいはコピーしたＩＣカードが使用された可

能性があると判断する。ことを特徴とするものである。これにより、顧客管理センターは、番号通知サービスを利用して通知された電話番号と、顧客データベースに記憶されている顧客が所有する受信機に接続されている公衆電話回線の電話番号とが異なっている場合、同じID番号を有するICカードが、顧客が視聴契約した時に登録した場所とは別の場所で使用されたことになり、その結果、偽造あるいはコピーしたICカードが使用されたと判断し、不正視聴を発見可能な有料放送システムを実現することができる。

【0008】請求項2に係る有料放送システムは、請求項1に記載の有料放送システムにおいて、前記顧客管理センターは、前記顧客データベースに記憶されていない電話番号が通知された場合、あるいは、顧客データベースに記憶されていないID番号が送信された場合、偽造あるいはコピーしたICカードが使用された可能性があると判断する。ことを特徴とするものである。これにより、顧客管理センターは、顧客データベースに記憶されていない顧客情報を受信した場合、偽造あるいはコピーしたICカードが使用されたと判断し、不正視聴を発見できる。

【0009】請求項3に係る有料放送システムは、請求項1または請求項2に記載の有料放送システムにおいて、前記顧客管理センターは、前記偽造あるいはコピーしたICカードが使用された可能性があると判断した場合、不正視聴した受信機の場所を、前記番号通知サービスの利用により通知された電話番号に基づいて探索すること、を特徴とするものである。これにより、顧客管理センターは、偽造あるいはコピーしたICカードの使用による不正視聴を発見した場合、不正視聴した受信機より番号通知サービスを利用して通知された電話番号から発信元をつきとめることが可能である。

【0010】請求項4に係る有料放送システムは、請求項1ないし請求項3のいずれかに記載の有料放送システムにおいて、前記ICカードは読み出し専用で、該ICカードに記憶されているID番号は全ての顧客に対して固有のデータである。ことを特徴とするものである。これにより、有料放送データの視聴契約を締結した顧客を特定することができる。

【0011】請求項5に係る有料放送システムは、請求項1ないし請求項4のいずれかに記載の有料放送システムにおいて、前記ID番号として、前記ICカードの製造番号を使用する。ことを特徴とするものである。これにより、ICカードの製造番号はICカード固有の番号であり、有料放送データの視聴契約を締結した顧客を特定することができる。

【0012】請求項6に係る有料放送システムは、有料放送データを提供する放送局と視聴契約を締結した顧客が、該有料放送データを受信可能な受信機を設置して該有料放送データを視聴する有料放送システムにおいて、

有料放送データをエンコードするエンコーダと、前記エンコードされた有料放送データをスクランブル鍵によりスクランブルするスクランブラと、前記スクランブル鍵を発生するスクランブル鍵発生装置と、マスター鍵により前記スクランブル鍵を暗号化する暗号化装置と、前記暗号化されたスクランブル鍵と前記スクランブルされた有料放送データとを多重化する多重化装置と、前記多重化された有料放送データを送信する送信アンテナと、を具備する放送局と、前記放送局から通信衛星を介して前記多重化された有料放送データを受信する受信アンテナと、前記多重化された有料放送データに対して復調処理を施すチューナと、前記復調された有料放送データから前記暗号化されたスクランブル鍵及び前記スクランブルされた有料放送データを抽出し、前記スクランブルされた有料放送データに対してデスクランブル処理を施すデスクランブラ・デマルチプレクサと、前記デスクランブルされた有料放送データをデコードするデコーダと、前記放送局にて前記スクランブル鍵の暗号化処理に使用した前記マスター鍵と同一の情報を持つマスター鍵を有し、該マスター鍵を用いて前記デスクランブラ・デマルチプレクサにて抽出された前記暗号化されたスクランブル鍵に対して暗号化復号処理を施し、前記デスクランブル処理に必要なスクランブル鍵として前記デスクランブラ・デマルチプレクサへ出力するICカードと、公衆電話回線に接続可能なモデムと、を具備する受信機と、有料放送データの視聴契約時に、氏名、住所、ICカードに記憶されているマスター鍵情報、受信機に接続されている公衆電話回線の電話番号等の各顧客に関する顧客情報を記録管理し、前記マスター鍵情報を暗号化装置へ出力する顧客データベースと、前記顧客情報を必要に応じて照会する顧客照会装置と、を具備する顧客管理センターと、と構成され、前記顧客が前記有料放送データを視聴する場合あるいは視聴した場合、該顧客が所有する受信機は、番号通知サービスを利用して、前記顧客管理センターへ発呼を前記公衆電話回線を介して行い、視聴要求あるいは視聴結果とともに前記顧客のICカードに記憶されているマスター鍵情報を送信し、前記顧客管理センターは、前記ICカードに記憶されているマスター鍵情報及び前記番号通知サービスの利用により通知された電話番号と、前記顧客データベースに記憶されている前記顧客のマスター鍵情報及び前記顧客が所有する受信機に接続されている公衆電話回線の電話番号と、前記顧客情報照会装置にて照合し、前記照会の結果、前記顧客データベースに記憶されている前記顧客が所有する受信機に接続されている前記公衆電話回線の電話番号と前記番号通知サービスにより通知された電話番号とが異なる場合、偽造あるいはコピーしたICカードが使用された可能性があると判断する。ことを特徴とするものである。【0013】これにより、顧客管理センターでは、番号通知サービスを利用して通知された電話番号と、顧客デ

ータベースに記憶されている顧客が所有する受信機に接続されている公衆電話回線の電話番号とが異なっている場合、同じマスター鍵情報を有するＩＣカードが、顧客が視聴契約した時に登録した場所とは別の場所で使用されたことになり、その結果、偽造あるいはコピーしたＩＣカードが使用されたと判断することができ、また、ＩＣカードに記憶されているマスター鍵情報を顧客のＩＤ番号として使用することで、ＩＣカードに記憶する情報を減少でき、より低コストで不正視聴を発見可能な有料放送システムを実現できる。

【００１４】請求項７に係る有料放送システムは、請求項６に記載の有料放送システムにおいて、前記顧客管理センターは、前記顧客データベースに記憶されていない電話番号が通知された場合、あるいは、顧客データベースに記憶されていないマスター鍵情報が送信された場合、偽造あるいはコピーしたＩＣカードが使用された可能性があると判断する。ことを特徴とするものである。これにより、顧客管理センターでは、顧客データベースに記憶されていない顧客情報を受信した場合、偽造あるいはコピーしたＩＣカードが使用されたと判断し、不正視聴を発見できる。

【００１５】請求項８に係る有料放送システムは、請求項６または請求項７に記載の有料放送システムにおいて、前記顧客管理センターは、前記偽造あるいはコピーしたＩＣカードが使用された可能性があると判断した場合、不正視聴した受信機の場所を、前記番号通知サービスの利用により通知された電話番号に基づいて探索すること、を特徴とするものである。これにより、顧客管理センターは、偽造あるいはコピーしたＩＣカードの使用による不正視聴を発見した場合、不正視聴した受信機より番号通知サービスを利用して通知された電話番号から、発信元をつきとめることが可能である。

【００１６】請求項９に係る有料放送システムは、請求項６ないし請求項８のいずれかに記載の有料放送システムにおいて、前記ＩＣカードに記憶されている前記マスター鍵情報は、読出し専用で、かつ、全ての顧客に対して固有のデータである。ことを特徴とするものである。これにより、有料放送データの視聴契約を締結した顧客を特定することができる。

【００１７】請求項１０に係る有料放送システムは、有料放送データを提供する放送局と視聴契約を締結した顧客が、該有料放送データを受信可能な受信機を設置して該有料放送データを視聴する有料放送システムにおいて、有料放送データをエンコードするエンコードと、前記エンコードされた有料放送データをスクランブル鍵によりスクランブルするスクランブラと、前記スクランブル鍵とワーク鍵とを発生するスクランブル鍵発生装置と、前記スクランブル鍵を前記ワーク鍵により暗号化し、さらに、マスター鍵により前記ワーク鍵を暗号化する暗号化装置と、前記暗号化されたスクランブル鍵と前

記暗号化されたワーク鍵と前記スクランブルされた有料放送データとを多重化する多重化装置と、前記多重化された有料放送データを送信する送信アンテナと、を具備する放送局と、前記放送局から通信衛星を介して前記多重化された有料放送データを受信する受信アンテナと、前記受信アンテナにて受信した前記多重化された有料放送データに対して復調処理を施すチューナと、前記復調された有料放送データから前記暗号化されたスクランブル鍵と前記暗号化されたワーク鍵と前記スクランブルされた有料放送データとを抽出し、前記スクランブルされた有料放送データに対してデスクランブル処理を施すデスクランブラ・デマルチプレクサと、前記デスクランブルされた有料放送データをデコードするデコードと、前記放送局にて前記ワーク鍵の暗号化に使用した前記マスター鍵と同一の情報を保持するマスター鍵を有し、該マスター鍵を用いて前記デスクランブラ・デマルチプレクサにて抽出された前記暗号化されたワーク鍵に対して暗号化復号処理を施し、該復号化されたワーク鍵を記憶し、さらに、該ワーク鍵を用いて前記暗号化されたスクランブル鍵に対して暗号化復号処理を施し、前記デスクランブル処理に必要なスクランブル鍵として前記デスクランブラ・デマルチプレクサへ出力するＩＣカードと、公衆電話回線に接続可能なモデムと、を具備する受信機と、有料放送データの視聴契約時に、氏名、住所、ＩＣカードに記憶されているマスター鍵情報、該マスター鍵により暗号化あるいは暗号化復号処理されるワーク鍵情報、受信機に接続されている公衆電話回線の電話番号等の各顧客に関する顧客情報を記録管理し、前記スクランブル鍵発生装置にて発生した前記ワーク鍵を暗号化するための前記マスター鍵を暗号化装置へ出力する顧客データベースと、前記顧客情報を必要に応じて照会する顧客照会装置と、を具備する顧客管理センターと、で構成され、前記顧客が前記有料放送データの視聴する場合あるいは視聴した場合、該顧客が所有する受信機は、番号通知サービスを利用して、前記顧客管理センターへ発呼を前記公衆電話回線を介して行い、前記視聴要求あるいは前記視聴結果とともに前記ＩＣカードに記憶されたワーク鍵情報を前記顧客管理センターへ送信し、前記顧客管理センターは、前記送信されたワーク鍵情報及び前記番号通知サービスにより通知された電話番号と、前記顧客データベースに記憶されている前記顧客のワーク鍵情報及び前記顧客が所有する受信機に接続されている公衆電話回線の電話番号とを、前記顧客情報照会装置にて照会し、前記照会の結果、前記顧客データベースに記憶されている前記顧客が所有する受信機に接続されている前記公衆電話回線の電話番号と前記番号通知サービスの利用により通知された電話番号とが異なる場合、偽造あるいはコピーしたＩＣカードが使用されたと可能性があると判断すること、を特徴とするものである。

【００１８】これにより、顧客管理センターでは、番号

通知サービスを利用して通知された電話番号と、顧客データベースに記憶されている顧客が所有する受信機に接続されている公衆電話回線の電話番号とが異なっている場合、同じワーク鍵情報を有するＩＣカードが、顧客が視聴契約した時に登録した場所とは別の場所で使用したことになり、その結果、偽造あるいはコピーしたＩＣカードが使用されたと判断することができ、また、ＩＣカードに記憶されるワーク鍵情報を顧客のＩＤ番号として使用することで、ＩＣカードに記憶する情報量を減少でき、より低コストで不正視聴を発見可能な有料放送システムを実現できる。

【００１９】請求項１１に係る有料放送システムは、請求項１０に記載の有料放送システムにおいて、前記顧客管理センターは、前記顧客データベースに記憶されていない電話番号が通知された場合、あるいは、顧客データベースに記憶されていないワーク鍵情報が送信された場合、偽造あるいはコピーしたＩＣカードが使用された可能性があると判断する。ことを特徴とするものである。これにより、顧客管理センターでは、顧客データベースに記憶されていない顧客情報を受信した場合、偽造あるいはコピーしたＩＣカードが使用されたと判断し、不正視聴を発見できる。

【００２０】請求項１２に係る有料放送システムは、請求項１０または請求項１１に記載の有料放送システムにおいて、前記顧客管理センターは、前記偽造あるいはコピーしたＩＣカードが使用された可能性があると判断した場合、不正視聴した受信機の場所を、前記番号通知サービスの利用により通知された電話番号に基づいて探索する。ことを特徴とするものである。これにより、顧客管理センターは、偽造あるいはコピーしたＩＣカードの使用による不正視聴を発見した場合、不正視聴した受信機より番号通知サービスを利用して通知された電話番号から発信元をつきとめることが可能である。

【００２１】請求項１３に係る有料放送システムは、請求項１０ないし請求項１２のいずれかに記載の有料放送システムにおいて、前記ＩＣカードに記憶される前記ワーク鍵情報は、更新可能である。ことを特徴とするものである。これにより、ワーク鍵情報を定期的に更新することで、有料放送システムのセキュリティを高めることができる。

【００２２】

【発明の実施の形態】以下に、本実施の形態について図面を参照しながら説明する。なお、ここで示す実施の形態はあくまでも一例であって、必ずしもこの実施の形態に限定されるものではない。

【００２３】（実施の形態１）以下に、実施の形態１に係る有料放送システムについて図面を参照しながら説明する。実施の形態１は、本発明の請求項１、請求項２、請求項３、及び請求項４に対応するものである。

【００２４】図１は、本発明の実施の形態１に係る有料

放送システムを示す図である。図１において、１０３は放送局であり、有料放送データをエンコードしてスクランブルするエンコーダ１０１と、エンコーダ１０１にてスクランブルされた有料放送データを送信する送信アンテナ１０２とを、具備するものである。

【００２５】１０９は受信機群であり、複数の各顧客が持つ受信機１０８からなる。各受信機１０８は、放送局１０３から通信衛星１０４を介してスクランブルされた有料放送データを受信する受信アンテナ１０５と、受信アンテナ１０５にて受信したスクランブルされた有料放送データに対してデスクランブル処理を施し、デコードするデコーダ１１５と、デスクランブル処理に必要な制御情報及び顧客を特定するためのＩＤ番号を記憶しているＩＣカード１０６と、公衆電話回線１１０に接続可能なモデム１０７とを、具備するものである。

【００２６】１１４は顧客管理センターであり、顧客情報１１１を記録管理する顧客データベース１１２と、顧客情報１１１を必要に応じて照会する顧客情報照会装置１１３とを、具備するものである。

【００２７】なお、顧客とは、放送局１０３と有料放送データの視聴契約を締結したユーザのことである。また、ＩＣカード１０６は読出し専用で、該ＩＣカード１０６に記憶されているＩＤ番号は全ての顧客に対して固有のデータであり、有料放送データの視聴契約を締結した顧客を特定することができる。

【００２８】次に、上記のように構成した有料放送システムにおいて、顧客が受信機で有料放送データを視聴する際のシステム動作について説明する。有料放送データの視聴契約時に、顧客であるユーザＡ～Ｚの氏名、住所、受信機Ａ～ＺのＩＣカードに記憶されているＩＤ番号「１１１～ＮＮＮ」、各ユーザが所有する受信機Ａ～Ｚのモデム１０７に接続されている公衆電話回線１１０の電話番号等の各顧客に関する顧客情報１１１を顧客データベース１１２に記録管理する。

【００２９】顧客が有料放送データを視聴する場合、顧客が所有する受信機１０８は、番号通知サービスを利用して、顧客管理センター１１４へ発呼を公衆電話回線１１０を介して行い、視聴要求及びＩＣカード１０６に記憶されているＩＤ番号を送信する。また、有料放送データを視聴した場合、顧客が所有する受信機１０８は、番号通知サービスを利用して、顧客管理センター１１４へ発呼を公衆電話回線１１０を介して行い、視聴結果及びＩＣカード１０６に記憶されているＩＤ番号を送信する。

【００３０】そして、顧客管理センター１１４は、受信機１０８より受信したＩＤ番号及び番号通知サービスの利用により通知された電話番号と、顧客データベース１１２に記憶されている顧客のＩＤ番号及び顧客が所有する受信機１０８に接続されている公衆電話回線１１０の電話番号とを、顧客情報照会装置１１３にて照合する。

【0031】そして、照合の結果、顧客データベース112に記憶されている顧客が所有する受信機108に接続されている公衆電話回線110の電話番号と、番号通知サービスの利用により通知された電話番号とが異なる場合、同じID番号を有するICカードが、顧客が視聴契約した時に登録した場所とは別の場所で使用されたことになり、偽造、あるいはコピーしたICカードが使用された可能性があると判断する。また、顧客データベース112に記憶されていない電話番号が通知された場合や顧客データベース112に記憶されていないID番号が送信された場合も、偽造あるいはコピーしたICカードが使用された可能性があると判断する。さらに、偽造あるいはコピーしたICカードが使用された可能性がある場合、顧客管理センター114は、不正視聴した受信機の場所を番号通知サービスの利用により通知された電話番号に基づいて探索し、発信元をつきとめることも可能である。

【0032】このような本実施の形態1による有料放送システムでは、顧客が有料放送データを視聴する場合あるいは視聴した場合、顧客が所有する受信機108は、番号通知サービスを利用して、視聴要求あるいは視聴結果とともにICカード106に記憶されているID番号を顧客管理センター114へ送信し、顧客管理センター114では、受信したID番号及び番号通知サービスの利用により通知された電話番号と、顧客データベース112に記憶されている顧客情報111と、を顧客情報照会装置113にて照合するようにしたので、顧客管理センター114は、番号通知サービスを利用して通知された電話番号と、顧客データベース112に記憶されている顧客が所有する受信機108に接続されている公衆電話回線110の電話番号とが異なる場合、同じID番号を有するICカード106が、顧客が視聴契約した時に登録した場所とは別の場所で使用されたことになり、その結果、偽造あるいはコピーしたICカードが使用されたことと判断し、不正視聴を発見可能な有料放送システムを実現することができる。さらに、顧客データベース112に記憶されていない顧客情報を受信した場合も、偽造あるいはコピーしたICカード106が使用されたことと判断し、不正視聴を発見できる。

【0033】また、顧客管理センター114は、偽造あるいはコピーしたICカード106が使用された可能性がある場合、不正視聴した受信機の場所を番号通知サービスの利用により通知された電話番号に基づいて探索するようにしたので、不正視聴した受信機の発信元をつきとめることができる。

【0034】(実施の形態2)以下に、実施の形態2に係る有料放送システムについて図面を参照しながら説明する。実施の形態2は、本発明の請求項1、請求項2、請求項3、請求項4、及び請求項5に対応するものである。

【0035】図2は、本発明の実施の形態2に係る有料放送システムを示す図である。図2において、206は放送局であり、有料放送データをエンコードしてスクランブルするエンコーダ204と、エンコーダ204にてスクランブルされた有料放送データを送信する送信アンテナ205とを、具備するものである。

【0036】212は受信機であり、放送局206から通信衛星207を介してスクランブルされた有料放送データを受信する受信アンテナ208と、受信アンテナにて受信したスクランブルされた有料放送データに対してデスクランブル処理を施し、デコードするチューナ・デコーダ209と、デスクランブル処理に必要な制御情報及び顧客を特定するためのID番号を記憶しているICカード210と、公衆電話回線213に接続可能なモデム211と、を具備するものである。ここで、ID番号は、ICカード210の製造番号を使用するものとする。

【0037】203は顧客管理センターであり、顧客情報を記録管理する顧客データベース201と、顧客情報を必要に応じて照会する顧客情報照会装置202と、を具備するものである。

【0038】なお、顧客とは、放送局206と有料放送データの視聴契約を締結したユーザのことである。また、ICカード210は読出し専用で、該ICカード210に記憶されているID番号は全ての顧客に対して固有のデータであり、有料放送データの視聴契約を知結した顧客を特定することができる。

【0039】次に、上記のように構成した有料放送システムにおいて、顧客が受信機で有料放送データを視聴する際のシステム動作について説明する。有料放送データの視聴契約時に、氏名、住所、ICカード210の製造番号、各ユーザが所有する受信機212のモデム211に接続されている公衆電話回線213の電話番号等の各顧客に関する顧客情報を顧客データベース201に記録管理する。

【0040】顧客が有料放送データを視聴する場合、顧客が所有する受信機212は、番号通知サービスを利用して、顧客管理センター203へ発呼を公衆電話回線213を介して行い、視聴要求及びICカード210の製造番号を送信する。また、有料放送データした場合、顧客が所有する受信機212は、番号通知サービスを利用して、顧客管理センター203へ発呼を公衆電話回線213を介して行い、視聴結果及びICカード210の製造番号を送信する。

【0041】そして、顧客管理センター203は、受信機212より受信したICカード210の製造番号及び番号通知サービスの利用により通知された電話番号と、顧客データベース201に記憶されている顧客のICカードの製造番号及び顧客が所有する受信機212に接続されている公衆電話回線213の電話番号と、を顧客情



報照会装置202にて照合する。

【0042】そして、照合の結果、顧客データベース201に記憶されている顧客が所有する受信機212に接続されている公衆電話回線213の電話番号と、番号通知サービスを利用して受信機212より通知された電話番号とが異なる場合、同じ製造番号を有するICカードが、顧客が視聴契約した時に登録した場所とは別の場所で使用されたことになり、偽造、あるいはコピーしたICカードが使用された可能性があると判断する。また、顧客データベース201に記憶されていない電話番号が通知された場合や顧客データベース201に記憶されていないICカードの製造番号が送信された場合も、偽造あるいはコピーしたICカードが使用された可能性があると判断する。さらに、偽造あるいはコピーしたICカードが使用された可能性があるとは判断した場合、顧客管理センター203は、不正視聴した受信機の場所を、番号通知サービスの利用により通知された電話番号に基づいて探索し、発信元をつきとめることができる。

【0043】このような本実施の形態2による有料放送システムでは、顧客が有料放送データを視聴する場合あるいは視聴した場合、顧客が所有する受信機212は、番号通知サービスを利用して、視聴要求あるいは視聴結果とともにICカード210の製造番号を顧客管理センター203へ送信し、顧客管理センター203では、受信したICカード210の製造番号及び番号通知サービスの利用により通知された電話番号と、顧客データベース201に記憶されている顧客情報と、顧客情報照会装置202にて照合するようにしたので、顧客管理センター203は、番号通知サービスを利用して通知された電話番号と、顧客データベース201に記憶されている顧客が所有する受信機212に接続されている公衆電話回線213の電話番号とが異なる場合、同じ製造番号のICカード210が、顧客が視聴契約した時に登録した場所とは別の場所で使用されたことになり、その結果、偽造あるいはコピーしたICカード210が使用されたと判断し、不正視聴を発見可能な有料放送システムを実現することができる。さらに、顧客データベース201に記憶されていない顧客情報を受信した場合も、偽造あるいはコピーしたICカード210が使用されたと判断し、不正視聴を発見できる。

【0044】また、顧客管理センター203は、偽造あるいはコピーしたICカード210が使用された可能性があるとは判断した場合、不正視聴した受信機の場所を番号通知サービスの利用により通知された電話番号に基づいて探索するようにしたので、不正視聴した受信機の発信元をつきとめることができる。

【0045】(実施の形態3)以下に、実施の形態3に係る有料放送システムについて図面を参照しながら説明する。実施の形態3は、本発明の請求項6、請求項7、請求項8、及び請求項9に対応するものである。

【0046】図3は、本発明の実施の形態3に係る有料放送システムを示す図である。310は放送局であり、有料放送データをエンコードするエンコーダ304と、エンコードされた有料放送データをスクランブル鍵Ksによりスクランブルするスクランブラ307と、スクランブル鍵Ksを発生するスクランブル鍵発生装置305と、マスター鍵Kmによりスクランブル鍵Ksを暗号化する暗号化装置306と、暗号化されたスクランブル鍵Ks'とスクランブルされた有料放送データとを多重化する多重化装置308と、多重化された有料放送データを送信する送信アンテナ309と、を具備するものである。

【0047】318は受信機であり、放送局310から通信衛星311を介して多重化された有料放送データを受信する受信アンテナ312と、多重化された有料放送データに対して復調処理を施すチューナ313と、復調された有料放送データから暗号化されたスクランブル鍵Ks及びスクランブルされた有料放送データを抽出し、スクランブルされた有料放送データに対してデスクランブル処理を施すデスクランブラ・デマルチプレクサ314と、デスクランブルされた有料放送データをデコードするデコーダ315と、放送局310にてスクランブル鍵Ksの暗号化処理に使用したマスター鍵Kmと同一の情報を保持するマスター鍵Kmを有し、マスター鍵Kmを用いてデスクランブラ・デマルチプレクサ314にて抽出された暗号化されたスクランブル鍵Ks'に対して暗号化復号処理を施し、デスクランブル処理に必要なスクランブル鍵Ksとてデスクランブラ・デマルチプレクサ314へ出力するICカード316と、公衆電話回線319に接続可能なモデム317と、を具備するものである。

【0048】303は顧客管理センターであり、顧客情報を記録管理し、マスター鍵Km情報を暗号化装置306へ出力する顧客データベース301と、顧客情報を必要に応じて照会する顧客照会装置302と、を具備するものである。

【0049】なお、顧客とは、放送局310と有料放送データの視聴契約を締結したユーザーのことである。また、ICカード316に記憶されているマスター鍵Ks情報は、読出し専用で、かつ、全ての顧客に対して固有のデータである。また、ICカード316に記憶されているマスター鍵Km情報はID番号として使用することで、ICカード316に記憶する情報量を減少できる。

【0050】次に、上記のように構成した有料放送システムにおいて、顧客が受信機で有料放送データを視聴する際のシステム動作について説明する。有料放送データの視聴契約時に、氏名、住所、ICカード316に記憶されているマスター鍵Ks情報、受信機318に接続されている公衆電話回線319の電話番号等の各顧客に関する顧客情報を顧客データベース301に記録管理す

る。

【0051】顧客が有料放送データを視聴する場合、顧客が所有する受信機318は、番号通知サービスを利用して、顧客管理センター303へ発呼を公衆電話回線319を介して行い、視聴要求及び顧客のICカード316に記憶されているマスター鍵Km情報を送信する。また、顧客が有料放送データを視聴した場合、顧客が所有する受信機318は、番号通知サービスを利用して、顧客管理センター303へ発呼を公衆電話回線319を介して行い、視聴結果及び顧客のICカード316に記憶されているマスター鍵Km情報を送信する。

【0052】そして、顧客管理センター303は、受信機318より受信したマスター鍵Km情報及び番号通知サービスの利用により通知された電話番号と、顧客データベース301に記憶されている顧客のマスター鍵Km情報及び顧客が所有する受信機318に接続されている公衆電話回線319の電話番号と、顧客情報照会装置302にて照合する。

【0053】そして、照合の結果、顧客データベース301に記憶されている顧客が所有する受信機318に接続されている公衆電話回線319の電話番号と番号通知サービスの利用により通知された電話番号とが異なる場合、偽造あるいはコピーしたICカードが使用された可能性があると判断する。また、顧客データベース301に記憶されていない電話番号が通知された場合や顧客データベース301に記憶されているID番号が送信された場合も、偽造あるいはコピーしたICカードが使用された可能性があると判断する。さらに、偽造あるいはコピーしたICカードが使用された可能性があると判断した場合、顧客管理センター303は、不正視聴した受信機の場所を、番号通知サービスの利用により通知された電話番号に基づいて探索し、発信元をつきとめることも可能である。

【0054】このような本実施の形態3による有料放送システムでは、顧客が有料放送データを視聴する場合あるいは視聴した場合、顧客が所有する受信機318は、番号通知サービスを利用して、視聴要求あるいは視聴結果とともにICカード316に記憶されているマスター鍵Km情報を顧客管理センター303へ送信し、顧客管理センター303では、受信したマスター鍵Km情報及び番号通知サービスの利用により通知された電話番号と、顧客データベース301に記憶されている顧客情報と、顧客情報照会装置302にて照合するようにしたので、顧客管理センター303は、番号通知サービスを利用して通知された電話番号と、顧客データベース301に記憶されている顧客が所有する受信機318に接続されている公衆電話回線319の電話番号とが異なっている場合、同じマスター鍵Km情報を有するICカード316が、顧客が視聴契約した時に登録した場所とは別の場所で使用されたことになり、その結果、偽造あるい

はコピーしたICカード316が使用されたと判断し、不正視聴を発見可能な有料放送システムを実現することができる。さらに、顧客データベース301に記憶されていない顧客情報を受信した場合も、偽造あるいはコピーしたICカード316が使用されたと判断し、不正視聴を発見できる。

【0055】また、顧客管理センター303は、偽造あるいはコピーしたICカード316が使用された可能性があるとして判断した場合、不正視聴した受信機の場所を番号通知サービスの利用により通知された電話番号に基づいて探索するようにしたので、不正視聴した受信機の発信元をつきとめることができる。

【0056】(実施の形態4)以下に、実施の形態4に係る有料放送システムについて図面を参照しながら説明する。実施の形態4は、本発明の請求項10、請求項11、請求項12、及び請求項13に対応するものである。

【0057】図4は、本実施の形態4に係る有料放送システムを示す図である。410は放送局であり、有料放送データをエンコードするエンコーダ404と、エンコードされた有料放送データをスクランブル鍵Ksによりスクランブルするスクランブラ407と、スクランブル鍵Ksとワーク鍵Kwとを発生するスクランブル鍵発生装置405と、ワーク鍵Kwによりスクランブル鍵Ksを暗号化し、さらに、マスター鍵Kmによりワーク鍵Kwを暗号化する暗号化装置406と、暗号化されたスクランブル鍵Ks'と暗号化されたワーク鍵Kw'とスクランブルされた有料放送データとを多重化する多重化装置408と、多重化された有料放送データを送信する送信アンテナ409と、を具備するものである。

【0058】418は受信機であり、放送局410から通信衛星419を介して多重化された有料放送データを受信する受信アンテナ412と、受信アンテナ412にて受信した多重化された有料放送データに対して復調処理を施すチューナ413と、復調された有料放送データから暗号化されたスクランブル鍵Ks'と暗号化されたワーク鍵Kw'とスクランブルされた有料放送データとを抽出し、スクランブルされた有料放送データに対してデスクランブル処理を施すデスクランブラ・デマルチプレクサ414と、デスクランブルされた有料放送データをデコードするデコーダ415と、放送局410にてワーク鍵Kwの暗号化に使用したマスター鍵Kmと同一の情報を持つマスター鍵Kmを有し、該マスター鍵Kmを用いてデスクランブラ・デマルチプレクサ414にて抽出された暗号化されたワーク鍵Kw'に対し暗号化復号処理を施し、該復号化されたワーク鍵Kwを記憶し、さらに、該ワーク鍵Kwを用いて暗号化されたスクランブル鍵Ks'に対し暗号化復号処理を施し、デスクランブル処理に必要なスクランブル鍵Ksとしてデスクランブラ・デマルチプレクサ414へ出力するICカード416

と、公衆電話回線419に接続可能なモデム417と、を具備するものである。

【0059】403は顧客管理センターであり、顧客情報を記録管理し、スクランブル鍵発生装置405にて発生したワーク鍵Kwを暗号化するためのマスター鍵Kmを暗号化装置406へ出力する顧客データベース401と、顧客情報を必要に応じて照会する顧客照会装置402と、を具備するものである。

【0060】なお、顧客とは、放送局410と有料放送データの視聴契約を締結したユーザのことである。また、ICカード416に記憶されるワーク鍵Kw情報をID番号として使用することで、ICカードに記憶する情報量を減少できる。また、ICカード416に記憶されるワーク鍵Kw情報は、更新可能である。

【0061】次に、上記のように構成した有料放送システムにおいて、顧客が受信機で有料放送データを視聴する際のシステム動作について説明する。有料放送データの視聴契約時に、氏名、住所、ICカードに記憶されているマスター鍵Km情報、該マスター鍵Kmにより暗号化あるいは暗号化復号処理されるワーク鍵Kw情報、受信機418に接続されている公衆電話回線419の電話番号等の各顧客に関する顧客情報を顧客データベース401に記録管理する。

【0062】顧客が有料放送データの視聴する場合、顧客が所有する受信機418は、番号通知サービスを利用して、顧客管理センター403へ発呼を公衆電話回線419を介して行い、視聴要求及びICカード416に記憶されたワーク鍵Kw情報を顧客管理センター403へ送信する。顧客が有料放送データの視聴した場合、顧客が所有する受信機418は、番号通知サービスを利用して、顧客管理センター403へ発呼を公衆電話回線419を介して行い、視聴結果及びICカード416に記憶されたワーク鍵Kw情報を顧客管理センター403へ送信する。

【0063】顧客管理センターは、受信機418より受信したワーク鍵Kw情報及び番号通知サービスの利用により通知された電話番号と、顧客データベース403に記憶されている顧客のワーク鍵Kw情報及び顧客が所有する受信機418に接続されている公衆電話回線419の電話番号とを、顧客情報照会装置402にて照会する。

【0064】そして、照会の結果、顧客データベース401に記憶されている顧客が所有する受信機418に接続されている公衆電話回線419の電話番号と番号通知サービスの利用により通知された電話番号とが異なる場合、偽造あるいはコピーしたICカードが使用された可能性があると判断する。また、顧客データベース201に記憶されていない電話番号が通知された場合や顧客データベース201に記憶されていないワーク鍵Kw情報が送信された場合も、偽造あるいはコピーしたICカード

が使用された可能性があると判断する。さらに、偽造あるいはコピーしたICカードが使用された可能性があると判断した場合、顧客管理センター303は、不正視聴した受信機の場所を、番号通知サービスの利用により通知された電話番号に基づいて探索し、発信元をつきとめることも可能である。

【0065】このような本実施の形態4による有料放送システムでは、顧客が有料放送データを視聴する場合あるいは視聴した場合、顧客が所有する受信機418は、番号通知サービスを利用して、視聴要求あるいは視聴結果とともにICカード416に記憶されたワーク鍵Kw情報を顧客管理センター403へ送信し、顧客管理センター403では、受信したワーク鍵Kw情報及び番号通知サービスの利用により通知された電話番号と、顧客データベース401に記憶されている顧客情報とを、顧客情報照会装置402にて照会するようにしたので、顧客管理センター403は、番号通知サービスを利用して通知された電話番号と、顧客データベース401に記憶されている顧客が所有する受信機418に接続されている公衆電話回線419の電話番号とが異なる場合はコピーしたICカード416が使用されたと判断し、不正視聴を発見可能な有料放送システムを実現することができる。さらに、顧客データベース401に記憶されていない顧客情報を受信した場合も、偽造あるいはコピーしたICカード416が使用されたと判断し、不正視聴を発見できる。

【0066】また、顧客管理センター403は、偽造あるいはコピーしたICカード416が使用された可能性があると判断した場合、不正視聴した受信機の場所を番号通知サービスの利用により通知された電話番号に基づいて探索するようにしたので、不正視聴した受信機の発信元をつきとめることができる。また、ワーク鍵Kw情報を定期的に更新することで、有料放送システムのセキュリティを高めることができる。

【0067】

【発明の効果】本発明の請求項1に記載の有料放送システムによれば、有料放送データを提供する放送局と視聴契約を締結した顧客が、該有料放送データを受信可能な受信機を設置して該有料放送データを視聴する有料放送システムにおいて、有料放送データを受信することで、スクランブルするエンコードと、前記スクランブルされた有料放送データを送信する送信アンテナと、を具備する放送局と、前記放送局から通信衛星を介して前記スクランブルされた有料放送データを受信する受信アンテナと、前記受信アンテナにて受信した前記スクランブルされた有料放送データに対してデスクランブル処理を施し、デコードするデコードと、前記デスクランブル処理

に必要な制御情報及び前記顧客を特定するためのID番号を記憶しているICカードと、公衆電話回線に接続可能なモデムと、を具備する受信機と、有料放送データの視聴契約時に、氏名、住所、ICカードのID番号、受信機に接続されている公衆電話回線の電話番号等の各顧客に関する顧客情報を記録管理する顧客データベースと、前記顧客情報を必要に応じて照会する顧客照会装置と、を具備する顧客管理センターと、で構成され、前記顧客が前記有料放送データを視聴する場合あるいは視聴した場合、該顧客が所有する受信機は、番号通知サービスを利用して、前記顧客管理センターへ発信を前記公衆電話回線を介して行い、視聴要求あるいは視聴結果とともに前記顧客のICカードに記憶されているID番号を前記顧客管理センターへ送信し、前記顧客管理センターは、前記受信したID番号及び前記番号通知サービスの利用により通知された電話番号と、前記顧客データベースに記憶されている前記顧客のID番号及び前記顧客が所有する受信機に接続されている公衆電話回線の電話番号と、を前記顧客情報照会装置に照会することにより、顧客管理センターは、番号通知サービスを利用して通知された電話番号と、顧客データベースに記憶されている顧客が所有する受信機に接続されている公衆電話回線の電話番号とが異なっている場合、同じID番号を有するICカードが、顧客が視聴契約した時に登録した場所とは別の場所で使用されたことになり、その結果、偽造あるいはコピーしたICカードが使用されたと判断し、不正視聴を発見可能な有料放送システムを実現することができる。

【0068】請求項2に記載の有料放送システムによれば、請求項1に記載の有料放送システムにおいて、前記顧客管理センターは、前記顧客データベースに記憶されていない電話番号が通知された場合、あるいは、顧客データベースに記憶されていないID番号が送信された場合、偽造あるいはコピーしたICカードが使用された可能性があると判断するようにしたので、顧客管理センターでは、顧客データベースに記憶されていない顧客情報を受信した場合に偽造あるいはコピーしたICカードが使用されたと判断し、不正視聴を発見可能な有料放送システムを実現できる。

【0069】請求項3に記載の有料放送システムによれば、請求項1または請求項2に記載の有料放送システムにおいて、前記顧客管理センターは、前記偽造あるいはコピーしたICカードが使用された可能性があると判断した場合、不正視聴した受信機の場所を、前記番号通知サービスの利用により通知された電話番号に基づいて探索するようにしたので、顧客管理センターは、偽造あるいはコピーしたICカードの使用による不正視聴を発見した場合、不正視聴した受信機より番号通知サービスを利用して通知された電話番号から発信元をつきとめることが可能である。

【0070】請求項4に記載の有料放送システムによれば、請求項1ないし請求項3のいずれかに記載の有料放送システムにおいて、前記ICカードは読み出し専用で、該ICカードに記憶されているID番号は全ての顧客に対して固有のデータであることより、有料放送データの視聴契約を締結した顧客を特定することができる。

【0071】請求項5に記載の有料放送システムによれば、請求項1ないし請求項4のいずれかに記載の有料放送システムにおいて、前記IC番号として前記ICカードの製造番号を使用することにより、ICカード固有の番号であるICカードの製造番号を基に、有料放送データの視聴契約を締結した顧客を特定することができる。

【0072】請求項6に記載の有料放送システムによれば、有料放送データを提供する放送局と視聴契約を締結した顧客が、該有料放送データを受信可能な受信機を設置して該有料放送データを視聴する有料放送システムにおいて、有料放送データをエンコードするエンコーダと、前記エンコードされた有料放送データをスクランブル鍵によりスクランブルするスクランブラと、前記スクランブル鍵を発生するスクランブル鍵発生装置と、マスター鍵により前記スクランブル鍵を暗号化する暗号化装置と、前記暗号化されたスクランブル鍵と前記スクランブルされた有料放送データとを多重化する多重化装置と、前記多重化された有料放送データを送信する送信アンテナと、を具備する放送局と、前記放送局と通信衛星を介して前記多重化された有料放送データを受信する受信アンテナと、前記多重化された有料放送データに対して復調処理を施すチューナと、前記復調された有料放送データから前記暗号化されたスクランブル鍵及び前記スクランブルされた有料放送データを抽出し、前記スクランブルされた有料放送データに対してデスクランブル処理を施すデスクランブラ・デマルチプレクサと、前記デスクランブルされた有料放送データをデコードするデコーダと、前記放送局にて前記スクランブル鍵の暗号化処理に使用した前記マスター鍵と同一の情報を持つマスター鍵を有し、該マスター鍵を用いて前記デスクランブラ・デマルチプレクサにて抽出された前記暗号化されたスクランブル鍵に対して暗号化復号処理を施し、前記デスクランブル処理に必要なスクランブル鍵として前記デスクランブラ・デマルチプレクサへ出力するICカードと、公衆電話回線に接続可能なモデムと、を具備する受信機と、有料放送データの視聴契約時に、氏名、住所、ICカードに記憶されているマスター鍵情報、受信機に接続されている公衆電話回線の電話番号等の各顧客に関する顧客情報を記録管理し、前記マスター鍵情報を暗号化装置へ出力する顧客データベースと、前記顧客情報を必要に応じて照会する顧客照会装置と、を具備する顧客管理センターと、で構成され、前記顧客が前記有料放送データを視聴する場合あるいは視聴した場合、該顧客が所有する受信機は、番号通知サービスを利用して、前記

顧客管理センターへ発呼を前記公衆電話回線を介して行い、視聴要求あるいは視聴結果とともに前記顧客のＩＣカードに記憶されているマスター鍵情報を送信し、前記顧客管理センターは、前記ＩＣカードに記憶されているマスター鍵情報及び前記番号通知サービスの利用により通知された電話番号と、前記顧客データベースに記憶されている前記顧客のマスター鍵情報及び前記顧客が所有する受信機に接続されている公衆電話回線の電話番号と、を前記顧客情報照会装置にて照合するようにしたので、顧客管理センターでは、番号通知サービスを利用して通知された電話番号と、顧客データベースに記憶されている顧客が所有する受信機に接続されている公衆電話回線の電話番号とが異なっている場合、同じマスター鍵情報を有するＩＣカードが、顧客が視聴契約した時に登録した場所とは別の場所で使用されたことになり、その結果、偽造あるいはコピーしたＩＣカードが使用されたと判断することができ、また、ＩＣカードに記憶されているマスター鍵情報を顧客のＩＤ番号として使用することで、ＩＣカードに記憶する情報量を減少でき、より低コストで不正視聴を発見可能な有料放送システムを実現できる。

【００７３】請求項７に記載の有料放送システムによれば、請求項６に記載の有料放送システムにおいて、前記顧客管理センターは、前記顧客データベースに記憶されていない電話番号が通知された場合、あるいは、顧客データベースに記憶されていないマスター鍵情報が送信された場合、偽造あるいはコピーしたＩＣカードが使用された可能性があると判断するようにしたので、顧客管理センターでは、顧客データベースに記憶されていない顧客情報を受信した場合に、偽造あるいはコピーしたＩＣカードが使用されたと判断し、不正視聴を発見できる。

【００７４】請求項８に記載の有料放送システムは、請求項６または請求項７に記載の有料放送システムにおいて、前記顧客管理センターは、前記偽造あるいはコピーしたＩＣカードが使用された可能性があると判断した場合、不正視聴した受信機の場所を、前記番号通知サービスの利用により通知された電話番号に基づいて探索するようにしたので、顧客管理センターは、偽造あるいはコピーしたＩＣカードの使用による不正視聴を発見した場合、不正視聴した受信機より番号通知サービスを利用して通知された電話番号から発信元をつきとめることが可能である。

【００７５】請求項９に記載の有料放送システムによれば、請求項６ないし請求項８のいずれかに記載の有料放送システムにおいて、前記ＩＣカードに記憶されている前記マスター鍵情報は、読出し専用で、かつ、全ての顧客に対して固有の前記データであることより、有料放送データの視聴契約を締結した顧客を特定することができる。

【００７６】請求項１０に記載の有料放送システムによれば、有料放送データを提供する放送局と視聴契約を締

結した顧客が、該有料放送データを受信可能な受信機を設置して該有料放送データを視聴する有料放送システムにおいて、有料放送データをエンコードするエンコーダと、前記エンコードされた有料放送データをスクランブル鍵によりスクランブルするスクランブラと、前記スクランブル鍵とワーク鍵とを発生するスクランブル鍵発生装置と、前記スクランブル鍵を前記ワーク鍵により暗号化し、さらに、マスター鍵により前記ワーク鍵を暗号化する暗号化装置と、前記暗号化されたスクランブル鍵と前記暗号化されたワーク鍵と前記スクランブルされた有料放送データとを多重化する多重化装置と、前記多重化された有料放送データを送信する送信アンテナと、を具備する放送局と、前記放送局から通信衛星を介して前記多重化された有料放送データを受信する受信アンテナと、前記受信アンテナにて受信した前記多重化された有料放送データに対して復調処理を施すチューナと、前記復調された有料放送データから前記暗号化されたスクランブル鍵と前記暗号化されたワーク鍵と前記スクランブルされた有料放送データとを抽出し、前記スクランブルされた有料放送データに対してデスクランブル処理を施すデスクランブラ・デマルチプレクサと、前記デスクランブルされた有料放送データをデコードするデコーダと、前記放送局にて前記ワーク鍵の暗号化に使用した前記マスター鍵と同一の情報を有するマスター鍵を有し、該マスター鍵を用いて前記デスクランブラ・デマルチプレクサにて抽出された前記暗号化されたワーク鍵に対して暗号化復号処理を施し、該復号化されたワーク鍵を記憶し、さらに、該ワーク鍵を用いて前記暗号化されたスクランブル鍵に対して暗号化復号処理を施し、前記デスクランブル処理に必要なスクランブル鍵として前記デスクランブラ・デマルチプレクサへ出力するＩＣカードと、公衆電話回線に接続可能なモデムと、を具備する受信機と、有料放送データの視聴契約時に、氏名、住所、ＩＣカードに記憶されているマスター鍵情報、該マスター鍵により暗号化あるいは暗号化復号処理されるワーク鍵情報、受信機に接続されている公衆電話回線の電話番号等の各顧客に関する顧客情報を記録管理し、前記スクランブル鍵発生装置にて発生した前記ワーク鍵を暗号化するための前記マスター鍵を暗号化装置へ出力する顧客データベースと、前記顧客情報を必要に応じて照会する顧客照会装置と、を具備する顧客管理センターと、で構成され、前記顧客が前記有料放送データの視聴する場合あるいは視聴した場合、該顧客が所有する受信機は、番号通知サービスを利用して、前記顧客管理センターへ発呼を前記公衆電話回線を介して行い、前記視聴要求あるいは前記視聴結果とともに前記ＩＣカードに記憶されたワーク鍵情報を前記顧客管理センターへ送信し、前記顧客管理センターは、前記送信されたワーク鍵情報及び前記番号通知サービスにより通知された電話番号と、前記顧客データベースに記憶されている前記顧客のワーク鍵情報及び

前記顧客が所有する受信機に接続されている公衆電話回線の電話番号と、を前記顧客情報照会装置にて照合するようにしたので、顧客管理センターでは、番号通知サービスを利用して通知された電話番号と、顧客データベースに記憶されている顧客が所有する受信機に接続されている公衆電話回線の電話番号とが異なっている場合、同じワーク鍵情報を有するＩＣカードが、顧客が視聴契約した時に登録した場所とは別の場所で使用されたことになり、その結果、偽造あるいはコピーしたＩＣカードが使用されたと判断することができ、また、ＩＣカードに記憶されるワーク鍵情報を顧客のＩＤ番号として使用することで、ＩＣカードに記憶する情報量を減少でき、より低コストで不正視聴を発見可能な有料放送システムを実現できる。

【００７】請求項１１に記載の有料放送システムによれば、請求項１０に記載の有料放送システムにおいて、前記顧客管理センターは、前記顧客データベースに記憶されていない電話番号が通知された場合、あるいは、顧客データベースに記憶されていないワーク鍵情報が送信された場合、偽造あるいはコピーしたＩＣカードが使用された可能性があると判断するようにしたので、顧客管理センターでは、顧客データベースに記憶されていない顧客情報を受信した場合に、偽造あるいはコピーしたＩＣカードが使用されたと判断し、不正視聴を発見できる。

【００８】請求項１２に記載の有料放送システムによれば、請求項１０または請求項１１に記載の有料放送システムにおいて、前記顧客管理センターは、前記偽造あるいはコピーしたＩＣカードが使用された可能性があるとして判断した場合、不正視聴した受信機の場所を、前記番号通知サービスの利用により通知された電話番号に基づいて探索するようにしたので、顧客管理センターは、偽造あるいはコピーしたＩＣカードの使用による不正視聴を発見した場合、不正視聴した受信機より番号通知サービスを利用して通知された電話番号から発信元をつきとめることが可能である。

【００９】請求項１３に記載の有料放送システムによれば、請求項１０ないし請求項１２のいずれかに記載の有料放送システムにおいて、前記ＩＣカードに記憶される前記ワーク鍵情報は、更新可能であることより、有料放送システムのセキュリティを高めることができる。

#### 【図面の簡単な説明】

【図１】本発明の実施の形態１に係る有料放送システムの構成図である。

【図２】本発明の実施の形態２に係る有料放送システムの構成図である。

【図３】本発明の実施の形態３に係る有料放送システムの構成図である。

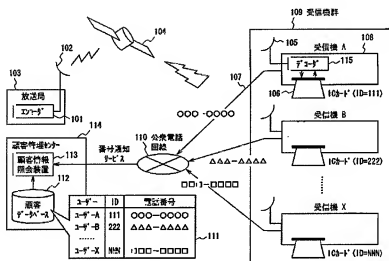
【図４】本発明の実施の形態４に係る有料放送システムの構成図である。

#### 【符号の説明】

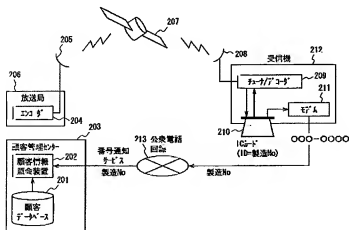
101	エンコーダ
102	送信アンテナ
103	放送局
104	通信衛星
105	受信アンテナ
106	ＩＣカード
107	モデム
108	受信機
109	受信機群
110	公衆電話回線
111	顧客情報
112	顧客データベース
113	顧客情報照会装置
114	顧客管理センター
115	デコーダ
201	顧客データベース
202	顧客情報照会装置
203	顧客管理センター
204	エンコーダ
205	送信アンテナ
206	放送局
207	通信衛星
208	受信アンテナ
209	チューナ・デコーダ
210	ＩＣカード
211	モデム
212	受信機
213	公衆電話回線
301	顧客データベース
302	顧客情報照会装置
303	顧客管理センター
304	エンコーダ
305	スクランブラ鍵発生装置
306	暗号化装置
307	スクランブラ
308	多重化装置
309	送信アンテナ
310	放送局
311	通信衛星
312	受信アンテナ
313	チューナ
314	デスクランブラ・デマルチプレクサ
315	デコーダ
316	ＩＣカード
317	モデム
318	受信機
319	公衆電話回線
401	顧客データベース
402	顧客情報照会装置

- |                 |                      |
|-----------------|----------------------|
| 403 顧客管理センター    | 412 受信アンテナ           |
| 404 エンコーダ       | 413 チューナ             |
| 405 スクランブル鍵発生装置 | 414 デスクランブラ・デマルチプレキサ |
| 406 暗号化装置       | 415 デコーダ             |
| 407 スクランプラ      | 416 ICカード            |
| 408 多重化装置       | 417 モデム              |
| 409 送信アンテナ      | 418 受信機              |
| 410 放送局         | 419 公衆電話回線           |
| 411 通信衛星        |                      |

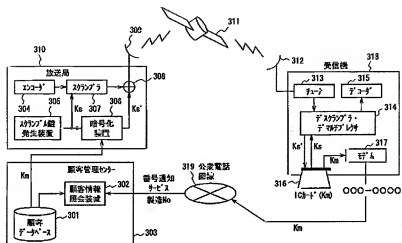
【図1】



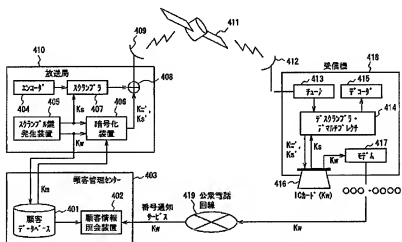
【図2】



【図3】



【図4】



フロントページの続き

(51) Int. Cl. 7

H 0 4 N 7/167

7/173

7/20

識別記号

6 1 0

6 1 0

F I

H 0 4 N 7/173

7/20

7/167

(参考)

6 1 0 Z

6 1 0

Z



## JP 2002-246996 PAJ machine translation

### DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the paid broadcasting system which used the satellite wave and the terrestrial wave for the intermediary roadway.

[0002]

[Description of the Prior Art] Now, digital-television-broadcasting service by the satellite wave or a terrestrial wave is offered all over the world. Only the customer who concluded the viewing-and-listening contract called CAS (Conditional Access System) can view and listen to a program, and the technical system prevent the other person from viewing and listening is introduced in paid broadcasting.

[0003] A signal is stirred in CAS and the art which enciphers the key for solving the scramble art and the scramble which are made for contents of broadcast not to be understood, and transmits is used for it. The scrambler which performs scramble processing changes the method of churning at any time, a malfeasance is kept from generating it, and the DEKUSU rumbler who cancels scramble cancels using the key used when applying scramble. Although a key is transmitted by a broadcast wave together with a program, since a malfeasance happens transmitting a key as it is easily, a key is enciphered and transmitted. A key is enciphered using another key (master key) at the transmitting side, and this master key is memorized by the IC card with which the televiewer who contracted is provided.

[0004] In CAS of digital television broadcasting, why the IC card is generally used, When the IC card forged or copied appears on the market, it is for consuming and stopping the damage over unjust viewing and listening by making unusable the IC card which was being used before the malfeasance was performed, and carrying out the recurrence line of the new IC card to each customer.

[0005]

[Problem(s) to be Solved by the Invention] However, the number of IC cards becomes so extensive [ the number of the IC cards by which a recurrence line is carried out ], when the IC card in which only the number of the customers who did the viewing-and-listening contract exists and which was sake [ the IC card ], forged or copied appears on the market.

[0006] This invention is made in order to cancel the above-mentioned problem, and it is a thing.

It is providing the paid broadcasting system which has a function which confirms at any time whether the purpose is performed or not.

[0007]

[Means for Solving the Problem] In order to solve an aforementioned problem, a paid broadcasting system concerning claim 1 of this invention, In a paid broadcasting system by which a customer who concluded a broadcasting station which provides paid broadcasting data, and a viewing-and-listening contract installs a receiver which can receive this paid broadcasting data, and views and listens to this paid broadcasting data, An encoder which encodes and carries out the scramble of the paid broadcasting data, A transmission antenna which transmits said paid broadcasting data by which scramble was carried out, A broadcasting station to provide and a receiving antenna which receives said paid broadcasting data by which scramble was carried out via a communications satellite from said broadcasting station, A decoder which performs and decodes descrambling processing to said paid broadcasting data which was received with said receiving antenna, and by which scramble

was carried out, An IC card which has memorized an ID number for specifying control information required for said descrambling processing, and said customer, At the time of a receiver possessing a modem connectable with a dial-up line, and a viewing-and-listening contract of paid broadcasting data. it coming out with a customer-relations-management center possessing a customer database which records customer data about each customer, such as a name, an address, an ID number of an IC card, and a telephone number of a dial-up line connected to a receiver, and a customer inquiry unit which refers for said customer data if needed, being constituted, and, When [ in which said customer views and listens to said paid broadcasting data ] it case, or views and listens, a receiver which this customer owns, Call origination is performed via said dial-up line using number notice service to said customer-relations-management center, Transmit to said customer-relations-management center, and an ID number memorized by said customer's IC card with a viewing-and-listening demand or a viewing-and-listening result said customer-relations-management center, A telephone number notified by use of said ID number which received, and said number notice service, A telephone number of a dial-up line connected to a receiver which an ID number of said customer remembered by said customer database and said customer own, When a telephone number of said dial-up line connected to a receiver which is compared in the aforementioned customer-data inquiry unit, and said customer remembered by said customer database owns as a result of said collation differs from a telephone number notified by use of said number notice service, It is judged that an IC card forged or copied may have been used. A telephone number to which a customer-relations-management center was notified by this using number notice service, When telephone numbers of a dial-up line connected to a receiver which a customer remembered by customer database owns differ, It can judge that an IC card which it means that it had been used at a place other than a place which an IC card which has the same ID number registered when a customer did a viewing-and-listening contract, and was forged or copied as a result was used, and a paid broadcasting system which can discover unjust viewing and listening can be realized.

[0008]In the paid broadcasting system according to claim 1, a paid broadcasting system concerning claim 2 said customer-relations-management center, When a telephone number which is not memorized by said customer database is notified, it is judged that an IC card to which an ID number which is not memorized by customer database was transmitted and which was case [ an IC card ], forged or copied may have been used. Thereby, in a customer-relations-management center, it judges that an IC card which received customer data which are not memorized by customer database and which was case [ an IC card ], forged or copied was used, and unjust viewing and listening can be discovered.

[0009]In the paid broadcasting system according to claim 1 or 2, a paid broadcasting system concerning claim 3 said customer-relations-management center, When it is judged that said IC card forged or copied may have been used, a place of a receiver which carried out unjust viewing and listening is searched based on a telephone number to which it was notified by use of said number notice service. Thereby, the customer-relations-management center can trace a sending agency from a telephone number notified from a receiver which carried out unjust viewing and listening using number notice service, when unjust viewing and listening by use of an IC card forged or copied is discovered.

[0010]In the paid broadcasting system according to any one of claims 1 to 3, said IC card of a paid broadcasting system concerning claim 4 is read-only, and an ID number memorized by this IC card is characterized by what is been peculiar data to all the customers. Thereby, a customer who concluded a viewing-and-listening contract of paid broadcasting data can be specified.

[0011]In the paid broadcasting system according to any one of claims 1 to 4, a serial number of said IC card is used for a paid broadcasting system concerning claim 5 as said ID number.

Thereby, a serial number of an IC card is a number peculiar to an IC card, and can specify a customer who concluded a viewing-and-listening contract of paid broadcasting data.

[0012] In a paid broadcasting system which a paid broadcasting system concerning claim 6 installs a receiver with which a customer who concluded a broadcasting station which provides paid broadcasting data, and a viewing-and-listening contract can receive this paid broadcasting data, and views and listens to this paid broadcasting data, An encoder which encodes paid broadcasting data, and a scrambler which carries out the scramble of said encoded paid broadcasting data with a scramble key, A scramble key generator which generates said scramble key, and an enciphering device which enciphers said scramble key with a master key, A multiplexing device which multiplexes said enciphered scramble key and said paid broadcasting data by which scramble was carried out, A broadcasting station possessing a transmission antenna which transmits said multiplexed paid broadcasting data, A receiving antenna which receives said multiplexed paid broadcasting data via a communications satellite from said broadcasting station, A tuner which performs recovery processing to said multiplexed paid broadcasting data, A descrambler demultiplexer which extracts said enciphered SUKURAMBU key and said paid broadcasting data by which scramble was carried out from said paid broadcasting data to which it restored, and performs descrambling processing to said paid broadcasting data by which scramble was carried out, A decoder which decodes said descrambled paid broadcasting data, It has said master key used for encryption processing of said scramble key at said broadcasting station, and a master key with the same information, Encryption decoding processing is performed to said enciphered scramble key which was extracted in said descrambler demultiplexer using this master key, An IC card outputted to said descrambler demultiplexer as a scramble key required for said descrambling processing, At the time of a receiver possessing a modem connectable with a dial-up line, and a viewing-and-listening contract of paid broadcasting data. A customer database which records customer data about each customer, such as a telephone number etc. of a name, an address, master key information memorized by IC card, and a dial-up line connected to a receiver, and outputs said master key information to an enciphering device, A customer-relations-management center possessing a customer inquiry unit which refers for said customer data if needed, When [ in which it appears and it is constituted, and said customer views and listens to said paid broadcasting data ] it case, or views and listens, a receiver which this customer owns performs call origination via said dial-up line using number notice service to said customer-relations-management center, Transmit and master key information memorized by said customer's IC card with a viewing-and-listening demand or a viewing-and-listening result said customer-relations-management center, A telephone number notified by use of master key information memorized by said IC card and said number notice service, A telephone number of a dial-up line connected to a receiver which master key information of said customer remembered by said customer database and said customer own, When a telephone number of said dial-up line connected to a receiver which is compared in the aforementioned customer-data inquiry unit, and said customer remembered by said customer database owns as a result of said collation differs from a telephone number notified by said number notice service, It is judged that an IC card forged or copied may have been used.

[0013] A telephone number notified in the customer-relations-management center by this using number notice service, When telephone numbers of a dial-up line connected to a receiver which a customer remembered by customer database owns differ, It means that it was used at a place other than a place which an IC card which has the same master key information registered when a customer did a viewing-and-listening contract, By as a result, a thing for which master key information which can judge that an IC card forged or copied was used, and is memorized by IC card is used as a customer's ID number. The amount of

information memorized to an IC card can be decreased, and a paid broadcasting system which can discover unjust viewing and listening can be realized more by low cost.

[0014]In the paid broadcasting system according to claim 6, a paid broadcasting system concerning claim 7 said customer-relations-management center, When a telephone number which is not memorized by said customer database is notified, it is judged that an IC card to which master key information which is not memorized by customer database was transmitted and which was case [ an IC card ], forged or copied may have been used. Thereby, in a customer-relations-management center, it judges that an IC card which received customer data which are not memorized by customer database and which was case [ an IC card ], forged or copied was used, and unjust viewing and listening can be discovered.

[0015]In the paid broadcasting system according to claim 6 or 7, a paid broadcasting system concerning claim 8 said customer-relations-management center, When it is judged that said IC card forged or copied may have been used, a place of a receiver which carried out unjust viewing and listening is searched based on a telephone number to which it was notified by use of said number notice service. Thereby, the customer-relations-management center can trace a sending agency from a telephone number notified from a receiver which carried out unjust viewing and listening using number notice service, when unjust viewing and listening by use of an IC card forged or copied is discovered.

[0016]Said master key information a paid broadcasting system concerning claim 9 is remembered to be by said IC card in the paid broadcasting system according to any one of claims 6 to 8 is read-only, and is characterized by what is been peculiar data to all the customers. Thereby, a customer who concluded a viewing-and-listening contract of paid broadcasting data can be specified.

[0017]In a paid broadcasting system which a paid broadcasting system concerning claim 10 installs a receiver with which a customer who concluded a broadcasting station which provides paid broadcasting data, and a viewing-and-listening contract can receive this paid broadcasting data, and views and listens to this paid broadcasting data, An encoder which encodes paid broadcasting data, and a scrambler which carries out the scramble of said encoded paid broadcasting data with a scramble key, A scramble key generator which generates said scramble key and a work key, An enciphering device which enciphers said scramble key with said work key, and enciphers said work key with a master key further, A multiplexing device which multiplexes said enciphered scramble key, said enciphered work key, and said paid broadcasting data by which scramble was carried out, A broadcasting station possessing a transmission antenna which transmits said multiplexed paid broadcasting data, A receiving antenna which receives said multiplexed paid broadcasting data via a communications satellite from said broadcasting station, and a tuner which performs recovery processing to said multiplexed paid broadcasting data which was received with said receiving antenna, Said enciphered scramble key, said enciphered work key, and said paid broadcasting data by which Scramble was carried out are extracted from said paid broadcasting data to which it restored, A descrambler demultiplexer which performs descrambling processing to said paid broadcasting data by which scramble was carried out, A decoder which decodes said descrambled paid broadcasting data, It has said master key used for encryption of said work key at said broadcasting station, and a master key with the same information, Encryption decoding processing is performed to said enciphered work key which was extracted in said descrambler demultiplexer using this master key, Memorize a decrypted this work key and encryption decoding processing is further performed to said enciphered scramble key using this work key, An IC card outputted to said descrambler demultiplexer as a scramble key required for said descrambling processing, Master key information remembered to be a receiver possessing a modem connectable with a dial-up line by a name, an address, and IC card at the time of a viewing-and-listening contract of paid broadcasting data, work key

information by which encryption or encryption decoding processing is carried out with this master key, Customer data about each customer, such as a telephone number etc. of a dial-up line connected to a receiver, are recorded, A customer database which outputs said master key for enciphering said work key by which it was generated with said scramble key generator to an enciphering device, A customer-relations-management center possessing a customer inquiry unit which refers for said customer data if needed, Come out, are constituted, and when [ to which said paid broadcasting data views and listens ] it case, or views and listens, said customer a receiver which this customer owns, Call origination is performed via said dial-up line using number notice service to said customer-relations-management center, Transmit work key information memorized by said IC card with said viewing-and-listening demand or said viewing-and-listening result to said customer-relations-management center, and said customer-relations-management center, A telephone number notified by said transmitted work key information and said number notice service, Compare a telephone number of a dial-up line connected to a receiver which work key information of said customer remembered by said customer database and said customer own in said customer-data inquiry unit, and A result of said collation, When a telephone number of said dial-up line connected to a receiver which said customer remembered by said customer database owns differs from a telephone number notified by use of said number notice service, It is judged that an IC card forged or copied may have been used.

[0018]A telephone number notified in the customer-relations-management center by this using number notice service, When telephone numbers of a dial-up line connected to a receiver which a customer remembered by customer database owns differ, It means that it was used at a place other than a place which an IC card which has the same work key information registered when a customer did a viewing-and-listening contract, By as a result, a thing for which work key information which can judge that an IC card forged or copied was used, and is memorized by IC card is used as a customer's ID number. The amount of information memorized to an IC card can be decreased, and a paid broadcasting system which can discover unjust viewing and listening can be realized more by low cost.

[0019]In the paid broadcasting system according to claim 10, a paid broadcasting system concerning claim 11 said customer-relations-management center, When a telephone number which is not memorized by said customer database is notified, it is judged that an IC card to which work key information which is not memorized by customer database was transmitted and which was case [ an IC card ], forged or copied may have been used. Thereby, in a customer-relations-management center, it judges that an IC card which received customer data which are not memorized by customer database and which was case [ an IC card ], forged or copied was used, and unjust viewing and listening can be discovered.

[0020]In the paid broadcasting system according to claim 10 or 11, a paid broadcasting system concerning claim 12 said customer-relations-management center, When it is judged that said IC card forged or copied may have been used, a place of a receiver which carried out unjust viewing and listening is searched based on a telephone number to which it was notified by use of said number notice service. Thereby, the customer-relations-management center can trace a sending agency from a telephone number notified from a receiver which carried out unjust viewing and listening using number notice service, when unjust viewing and listening by use of an IC card forged or copied is discovered.

[0021]Said work key information a paid broadcasting system concerning claim 13 is remembered to be by said IC card in the paid broadcasting system according to any one of claims 10 to 12 is characterized by what can be updated. Thereby, security of a paid broadcasting system can be raised by updating work key information periodically.

[0022]

[Embodiment of the Invention]Below, it explains, referring to drawings for this embodiment.

The embodiment shown here is an example to the last, and is not necessarily limited to this embodiment.

[0023](Embodiment 1) Below, it explains, referring to drawings for the paid broadcasting system concerning Embodiment 1. Embodiment 1 corresponds to claim 1 of this invention, claim 2, claim 3, and claim 4.

[0024]Drawing 1 is a figure showing the paid broadcasting system concerning the embodiment of the invention 1. In drawing 1, 103 is a broadcasting station and possesses the encoder 101 which encodes and carries out the scramble of the paid broadcasting data, and the transmission antenna 102 which transmits the paid broadcasting data by which scramble was carried out with the encoder 101.

[0025]109 is a receiver group and consists of the receiver 108 which two or more customers of each have. The receiving antenna 105 which receives the paid broadcasting data in which the scramble of each receiver 108 was carried out via the communications satellite 104 from the broadcasting station 103, The decoder 115 which performs and decodes descrambling processing to the paid broadcasting data which was received with the receiving antenna 105, and by which scramble was carried out, IC card 106 which has memorized the ID number for specifying control information and a customer required for descrambling processing, and the modem 107 connectable with the dial-up line 110 are provided.

[0026]114 is a customer-relations-management center and possesses the customer database 112 which records the customer data 111, and the customer-data inquiry unit 113 which refers for the customer data 111 if needed.

[0027]A customer is the user who concluded the viewing-and-listening contract of the broadcasting station 103 and paid broadcasting data. IC card 106 is read-only, and to all the customers, the ID number memorized by this IC card 106 is peculiar data, and can specify the customer who concluded the viewing-and-listening contract of paid broadcasting data.

[0028]Next, in the paid broadcasting system constituted as mentioned above, the system action at the time of a customer viewing and listening to paid broadcasting data with a receiver is explained. The name of user A-X which is a customer at the time of the viewing-and-listening contract of paid broadcasting data, an address, The customer data 111 about each customer, such as an ID number "111 - NNN" memorized by the IC card of receiver A-X and a telephone number of the dial-up line 110 connected to the modem 107 of the receivers A-X which each user owns, are recorded in the customer database 112.

[0029]When a customer views and listens to paid broadcasting data, using number notice service, the receiver 108 which a customer owns performs call origination via the dial-up line 110 to the customer-relations-management center 114, and transmits the ID number memorized by the viewing-and-listening demand and IC card 106. When it views and listens to paid broadcasting data, using number notice service, the receiver 108 which a customer owns performs call origination via the dial-up line 110 to the customer-relations-management center 114, and transmits the ID number memorized by the viewing-and-listening result and IC card 106.

[0030]And the telephone number notified by use of the ID number which received the customer-relations-management center 114 from the receiver 108, and number notice service, The telephone number of the dial-up line 110 connected to the receiver 108 which a customer's ID number and customer who are remembered by the customer database 112 own is compared by the customer-data inquiry unit 113.

[0031]And the telephone number of the dial-up line 110 connected to the receiver 108 which the customer remembered by the customer database 112 owns as a result of collation, When the telephone numbers notified by use of number notice service differ, the IC card which has the same ID number judges that it means that it was used at somewhere else [ the place registered when a customer did a viewing-and-listening contract ], and the IC card forged or

copied may have been used. Also when the ID number memorized by neither the case where the telephone number which is not memorized by the customer database 112 is notified, nor the customer database 112 is transmitted, it is judged that the IC card forged or copied may have been used. When it is judged that the IC card forged or copied may have been used, the customer-relations-management center 114 can search the place of the receiver which carried out unjust viewing and listening based on the telephone number notified by use of number notice service, and can also trace a sending agency.

[0032]In the paid broadcasting system by such this Embodiment 1. When [ in which a customer views and listens to paid broadcasting data ] it case, or views and listens, the receiver 108 which a customer owns, Transmit to the customer-relations-management center 114 using number notice service, and the ID number memorized by IC card 106 with the viewing-and-listening demand or the viewing-and-listening result in the customer-relations-management center 114. Since the telephone number notified by use of the ID number which received, and number notice service, and the customer data 111 memorized by the customer database 112 were compared by the customer-data inquiry unit 113, The telephone number to which the customer-relations-management center 114 was notified using number notice service, When the telephone numbers of the dial-up line 110 connected to the receiver 108 which the customer remembered by the customer database 112 owns differ, It can judge that the IC card which it means that it had been used at the place other than the place which IC card 106 which has the same ID number registered when a customer did a viewing-and-listening contract, and was forged or copied as a result was used, and the paid broadcasting system which can discover unjust viewing and listening can be realized. Also when the customer data which are not memorized by the customer database 112 are received, it judges that IC card 106 forged or copied was used, and unjust viewing and listening can be discovered.

[0033]When it is judged that IC card 106 which forged or copied the customer-relations-management center 114 may have been used, Since the place of the receiver which carried out unjust viewing and listening was searched based on the telephone number notified by use of number notice service, dispatch-receiver which carried out unjust viewing and listening origin can be traced.

[0034](Embodiment 2) Below, it explains, referring to drawings for the paid broadcasting system concerning Embodiment 2. Embodiment 2 corresponds to claim 1 of this invention, claim 2, claim 3, claim 4, and claim 5.

[0035]Drawing 2 is a figure showing the paid broadcasting system concerning the embodiment of the invention 2. In drawing 2, 206 is a broadcasting station and possesses the encoder 204 which encodes and carries out the scramble of the paid broadcasting data, and the transmission antenna 205 which transmits the paid broadcasting data by which scramble was carried out with the encoder 204.

[0036]The receiving antenna 208 which receives the paid broadcasting data by which 212 is a receiver and scramble was carried out via the communications satellite 207 from the broadcasting station 206, The tuner decoder 209 which performs and decodes descrambling processing to the paid broadcasting data which was received with the receiving antenna, and by which scramble was carried out, IC card 210 which has memorized the ID number for specifying control information and a customer required for descrambling processing, and the modem 211 connectable with the dial-up line 213 are provided. Here, an ID number shall use the serial number of IC card 210.

[0037]203 is a customer-relations-management center and possesses the customer database 201 which records customer data, and the customer-data inquiry unit 202 which refers for customer data if needed.

[0038]A customer is the user who concluded the viewing-and-listening contract of the

broadcasting station 206 and paid broadcasting data. IC card 210 is read-only, and to all the customers, the ID number memorized by this IC card 210 is peculiar data, and can specify the customer who \*\*\*\*(ed) the viewing-and-listening contract of paid broadcasting data.

[0039]Next, in the paid broadcasting system constituted as mentioned above, the system action at the time of a customer viewing and listening to paid broadcasting data with a receiver is explained. At the time of the viewing-and-listening contract of paid broadcasting data, the customer data about each customer, such as a name, an address, a serial number of IC card 210, and a telephone number of the dial-up line 213 connected to the modem 211 of the receiver 212 which each user owns, are recorded in the customer database 201.

[0040]When a customer views and listens to paid broadcasting data, using number notice service, the receiver 212 which a customer owns performs call origination via the dial-up line 213 to the customer-relations-management center 203, and transmits the serial number of a viewing-and-listening demand and IC card 210. When paid broadcasting data is carried out, using number notice service, the receiver 212 which a customer owns performs call origination via the dial-up line 213 to the customer-relations-management center 203, and transmits the serial number of a viewing-and-listening result and IC card 210.

[0041]And the telephone number notified by the serial number of IC card 210 which received the customer-relations-management center 203 from the receiver 212, and use of number notice service, The telephone number of the dial-up line 213 connected to the receiver 212 which the serial number and customer of an IC card of a customer who are remembered by the customer database 201 own is compared by the customer-data inquiry unit 202.

[0042]And the telephone number of the dial-up line 213 connected to the receiver 212 which the customer remembered by the customer database 201 owns as a result of collation, When the telephone numbers notified from the receiver 212 using number notice service differ, The IC card which has the same serial number judges that it means that it was used at the place other than the place registered when a customer did a viewing-and-listening contract, and the IC card forged or copied may have been used. Also when the serial number of the IC card memorized by neither the case where the telephone number which is not memorized by the customer database 201 is notified, nor the customer database 201 is transmitted, it is judged that the IC card forged or copied may have been used. When it is judged that the IC card forged or copied may have been used, the customer-relations-management center 203 can search the place of the receiver which carried out unjust viewing and listening based on the telephone number notified by use of number notice service, and can trace a sending agency.

[0043]In the paid broadcasting system by such this Embodiment 2. When [ in which a customer views and listens to paid broadcasting data ] it case, or views and listens, the receiver 212 which a customer owns, Using number notice service, transmit to the customer-relations-management center 203 with a viewing-and-listening demand or a viewing-and-listening result, and the serial number of IC card 210 in the customer-relations-management center 203. Since the telephone number notified by the serial number of IC card 210 and the use of number notice service which were received, and the customer data memorized by the customer database 201 were compared by the customer-data inquiry unit 202, The telephone number to which the customer-relations-management center 203 was notified using number notice service, When the telephone numbers of the dial-up line 213 connected to the receiver 212 which the customer remembered by the customer database 201 owns differ, It can judge that IC card 210 which it means that it had been used at the place other than the place which IC card 210 of the same serial number registered when a customer did a viewing-and-listening contract, and was forged or copied as a result was used, and the paid broadcasting system which can discover unjust viewing and listening can be realized. Also when the customer data which are not memorized by the customer database 201 are received, it judges that IC card 210 forged or copied was used, and unjust viewing and listening can be discovered.



[0044]When it is judged that IC card 210 which forged or copied the customer-relations-management center 203 may have been used, Since the place of the receiver which carried out unjust viewing and listening was searched based on the telephone number notified by use of number notice service, dispatch-receiver which carried out unjust viewing and listening origin can be traced.

[0045](Embodiment 3) Below, it explains, referring to drawings for the paid broadcasting system concerning Embodiment 3. Embodiment 3 corresponds to claim 6 of this invention, claim 7, claim 8, and claim 9.

[0046]Drawing 3 is a figure showing the paid broadcasting system concerning the embodiment of the invention 3. The encoder 304 which 310 is a broadcasting station and encodes paid broadcasting data, The scrambler 307 which carries out the scramble of the encoded paid broadcasting data with the scramble key Ks, The scramble key generator 305 which generates the scramble key Ks, and the enciphering device 306 which enciphers the scramble key Ks with the master key Km, The multiplexing device 308 which multiplexes enciphered scramble key Ks' and the paid broadcasting data by which scramble was carried out, and the transmission antenna 309 which transmits the multiplexed paid broadcasting data are provided.

[0047]The receiving antenna 312 which receives the paid broadcasting data which 318 is a receiver and was multiplexed via the communications satellite 311 from the broadcasting station 310, The tuner 313 which performs recovery processing to the multiplexed paid broadcasting data, The SUKURAMBU key Ks and the paid broadcasting data by which scramble was carried out which were enciphered from the paid broadcasting data to which it restored are extracted, The descrambler demultiplexer 314 which performs descrambling processing to the paid broadcasting data by which scramble was carried out, The decoder 315 which decodes the descrambled paid broadcasting data, It has the master key Km used for encryption processing of the scramble key Ks at the broadcasting station 310, and the master key Km with the same information, Encryption decoding processing is performed to enciphered scramble key Ks' which was extracted by the descrambler demultiplexer 314 using the master key Km, IC card 316 outputted to the descrambler demultiplexer 314 as the scramble key Ks required for descrambling processing and the modem 317 connectable with the dial-up line 319 are provided.

[0048]303 is a customer-relations-management center, records customer data and possesses the customer database 301 which outputs master key Km information to the enciphering device 306, and the customer inquiry unit 302 which refers for customer data if needed.

[0049]A customer is the user who concluded the viewing-and-listening contract of the broadcasting station 310 and paid broadcasting data. The master key Ks information memorized by IC card 316 is read-only, and is peculiar data to all the customers. The amount of information memorized to IC card 316 can be decreased by using the master key Km information memorized by IC card 316 as an ID number.

[0050]Next, in the paid broadcasting system constituted as mentioned above, the system action at the time of a customer viewing and listening to paid broadcasting data with a receiver is explained. At the time of the viewing-and-listening contract of paid broadcasting data, the customer data about each customer, such as a telephone number etc. of the dial-up line 319 connected to a name, an address, the master key Ks information memorized by IC card 316, and the receiver 318, are recorded in the customer database 301.

[0051]When a customer views and listens to paid broadcasting data, using number notice service, the receiver 318 which a customer owns performs call origination via the dial-up line 319 to the customer-relations-management center 303, and transmits the master key Km information memorized by IC card 316 of the viewing-and-listening demand and the customer. When a customer views and listens to paid broadcasting data, using number notice

service, the receiver 318 which a customer owns performs call origination via the dial-up line 319 to the customer-relations-management center 303, and transmits the master key Km information memorized by IC card 316 of the viewing-and-listening result and the customer. [0052]And the telephone number notified by use of the master key Km information that the customer-relations-management center 303 was received from the receiver 318, and number notice service, The telephone number of the dial-up line 319 connected to the receiver 318 which a customer's master key Km information and customer who are remembered by the customer database 301 own is compared by the customer-data inquiry unit 302.

[0053]And when the telephone number of the dial-up line 319 connected to the receiver 318 which the customer remembered by the customer database 301 owns as a result of collation differs from the telephone number notified by use of number notice service, It is judged that the IC card forged or copied may have been used. Also when the ID number memorized by neither the case where the telephone number which is not memorized by the customer database 301 is notified, nor the customer database 301 is transmitted, it is judged that the IC card forged or copied may have been used. When it is judged that the IC card forged or copied may have been used, the customer-relations-management center 303 can search the place of the receiver which carried out unjust viewing and listening based on the telephone number notified by use of number notice service, and can also trace a sending agency.

[0054]In the paid broadcasting system by such this Embodiment 3. When [ in which a customer views and listens to paid broadcasting data ] it case, or views and listens, the receiver 318 which a customer owns, The master key Km information memorized by IC card 316 with the viewing-and-listening demand or the viewing-and-listening result is transmitted to the customer-relations-management center 303 using number notice service, The telephone number notified by use of the received master key Km information and number notice service in the customer-relations-management center 303, Since the customer data memorized by the customer database 301 were compared by the customer-data inquiry unit 302, the customer-relations-management center 303, When the telephone number notified using number notice service differs from the telephone number of the dial-up line 319 connected to the receiver 318 which the customer remembered by the customer database 301 owns, It means that it was used at the place other than the place which IC card 316 which has the same master key Km information registered when a customer did a viewing-and-listening contract, As a result, it can judge that IC card 316 forged or copied was used, and the paid broadcasting system which can discover unjust viewing and listening can be realized. Also when the customer data which are not memorized by the customer database 301 are received, it judges that IC card 316 forged or copied was used, and unjust viewing and listening can be discovered.

[0055]When it is judged that IC card 316 which forged or copied the customer-relations-management center 303 may have been used, Since the place of the receiver which carried out unjust viewing and listening was searched based on the telephone number notified by use of number notice service, dispatch-receiver which carried out unjust viewing and listening origin can be traced.

[0056](Embodiment 4) Below, it explains, referring to drawings for the paid broadcasting system concerning Embodiment 4. Embodiment 4 corresponds to claim 10 of this invention, claim 11, claim 12, and claim 13.

[0057]Drawing 4 is a figure showing the paid broadcasting system concerning this Embodiment 4. The encoder 404 which 410 is a broadcasting station and encodes paid broadcasting data, The scrambler 407 which carries out the scramble of the encoded paid broadcasting data with the scramble key Ks, The scramble key generator 405 which generates the scramble key Ks and the work key Kw, The enciphering device 406 which enciphers the scramble key Ks with the work key Kw, and enciphers the work key Kw with the master key Km further, The multiplexing device 408 which multiplexes work key Kw' enciphered as

enciphered scramble key Ks' and the paid broadcasting data by which scramble was carried out, and the transmission antenna 409 which transmits the multiplexed paid broadcasting data are provided.

[0058]The receiving antenna 412 which receives the paid broadcasting data which 418 is a receiver and was multiplexed via the communications satellite 419 from the broadcasting station 410, The tuner 413 which performs recovery processing to the multiplexed paid broadcasting data which was received with the receiving antenna 412, Work key Kw' enciphered as scramble key Ks' enciphered from the paid broadcasting data to which it restored, and the paid broadcasting data by which Scramble was carried out are extracted, The descrambler demultiplexer 414 which performs descrambling processing to the paid broadcasting data by which scramble was carried out, The decoder 415 which decodes the descrambled paid broadcasting data, It has the master key Km used for encryption of the work key Kw at the broadcasting station 410, and the master key Km with the same information, Encryption decoding processing is performed to enciphered work key Kw' which was extracted by the descrambler demultiplexer 414 using this master key Km, IC card 416 which memorizes the decrypted this work key Kw, performs encryption decoding processing further to scramble key Ks' enciphered using this work key Kw, and is outputted to the descrambler demultiplexer 414 as the scramble key Ks required for descrambling processing, The modem 417 connectable with the dial-up line 419 is provided.

[0059]The customer database 401 which outputs the master key Km for enciphering the work key Kw by which 403 is a customer-relations-management center, recorded customer data, and it was generated with the scramble key generator 405 to the enciphering device 406, The customer inquiry unit 402 which refers for customer data if needed is provided.

[0060]A customer is the user who concluded the viewing-and-listening contract of the broadcasting station 410 and paid broadcasting data. The amount of information memorized to an IC card can be decreased by using the work key Kw information memorized by IC card 416 as an ID number. The work key Kw information memorized by IC card 416 can be updated.

[0061]Next, in the paid broadcasting system constituted as mentioned above, the system action at the time of a customer viewing and listening to paid broadcasting data with a receiver is explained. The master key Km information memorized by the name, the address, and the IC card at the time of the viewing-and-listening contract of paid broadcasting data, The customer data about each customer, such as a telephone number etc. of the dial-up line 419 connected to the work key Kw information by which encryption or encryption decoding processing is carried out with this master key Km, and the receiver 418, are recorded in the customer database 401.

[0062]The work key Kw information that the receiver 418 which a customer owns when paid broadcasting data views and listens performed call origination via the dial-up line 419 using number notice service to the customer-relations-management center 403, and the customer was remembered by the viewing-and-listening demand and IC card 416 is transmitted to the customer-relations-management center 403. The work key Kw information that the receiver 418 which a customer owns when paid broadcasting data views and listens performed call origination via the dial-up line 419 using number notice service to the customer-relations-management center 403, and the customer was remembered by the viewing-and-listening result and IC card 416 is transmitted to the customer-relations-management center 403.

[0063]The telephone number notified by use of the work key Kw information that the customer-relations-management center was received from the receiver 418, and number notice service, The telephone number of the dial-up line 419 connected to the receiver 418 which a customer's work key Kw information and customer who are remembered by the customer database 403 own is compared by the customer-data inquiry unit 402.

[0064]And when the telephone number of the dial-up line 419 connected to the receiver 418 which the customer remembered by the customer database 401 owns as a result of collation differs from the telephone number notified by use of number notice service, It is judged that the IC card forged or copied may have been used. Also when the work key Kw information memorized by neither the case where the telephone number which is not memorized by the customer database 201 is notified, nor the customer database 201 is transmitted, it is judged that the IC card forged or copied may have been used. When it is judged that the IC card forged or copied may have been used, the customer-relations-management center 303 can search the place of the receiver which carried out unjust viewing and listening based on the telephone number notified by use of number notice service, and can also trace a sending agency.

[0065]In the paid broadcasting system by such this Embodiment 4. When [ in which a customer views and listens to paid broadcasting data ] it case, or views and listens, the receiver 418 which a customer owns, The work key Kw information memorized by IC card 416 with the viewing-and-listening demand or the viewing-and-listening result is transmitted to the customer-relations-management center 403 using number notice service, The telephone number notified by use of the received work key Kw information and number notice service in the customer-relations-management center 403, Since the customer data memorized by the customer database 401 were compared by the customer-data inquiry unit 402, the customer-relations-management center 403, When the telephone number notified using number notice service differs from the telephone number of the dial-up line 419 connected to the receiver 418 which the customer remembered by the customer database 401 owns, It can judge that IC card 416 which it means that it had been used at the place other than the place which IC card 416 which has the same work key Kw information registered when a customer did a viewing-and-listening contract, and was forged or copied as a result was used, and the paid broadcasting system which can discover unjust viewing and listening can be realized. Also when the customer data which are not memorized by the customer database 401 are received, it judges that IC card 416 forged or copied was used, and unjust viewing and listening can be discovered.

[0066]When it is judged that IC card 416 which forged or copied the customer-relations-management center 403 may have been used, Since the place of the receiver which carried out unjust viewing and listening was searched based on the telephone number notified by use of number notice service, dispatch-receiver which carried out unjust viewing and listening origin can be traced. The security of a paid broadcasting system can be raised by updating work key Kw information periodically.

[0067]

[Effect of the Invention]According to the paid broadcasting system of this invention according to claim 1, the customer who concluded the broadcasting station which provides paid broadcasting data, and the viewing-and-listening contract, In the paid broadcasting system which installs the receiver which can receive this paid broadcasting data, and views and listens to this paid broadcasting data, The encoder which encodes and carries out the scramble of the paid broadcasting data, The transmission antenna which transmits said paid broadcasting data by which scramble was carried out, The broadcasting station to provide and the receiving antenna which receives said paid broadcasting data by which scramble was carried out via a communications satellite from said broadcasting station, The decoder which performs and decodes descrambling processing to said paid broadcasting data which was received with said receiving antenna, and by which scramble was carried out, The IC card which has memorized the ID number for specifying control information required for said descrambling processing, and said customer, At the time of the receiver possessing a modem connectable with a dial-up line, and the viewing-and-listening contract of paid broadcasting

data. it coming out with the customer-relations-management center possessing the customer database which records the customer data about each customer, such as a name, an address, an ID number of an IC card, and a telephone number of the dial-up line connected to the receiver, and the customer inquiry unit which refers for said customer data if needed, being constituted, and, When [ in which said customer views and listens to said paid broadcasting data ] it case, or views and listens, the receiver which this customer owns, Call origination is performed via said dial-up line using number notice service to said customer-relations-management center, Transmit to said customer-relations-management center, and the ID number memorized by said customer's IC card with the viewing-and-listening demand or the viewing-and-listening result said customer-relations-management center, The telephone number notified by use of said ID number which received, and said number notice service, The telephone number of the dial-up line connected to the receiver which the ID number of said customer remembered by said customer database and said customer own, From comparing in the aforementioned customer-data inquiry unit, a customer-relations-management center, When the telephone number notified using number notice service differs from the telephone number of the dial-up line connected to the receiver which the customer remembered by the customer database owns, It can judge that the IC card which it means that it had been used at the place other than the place which the IC card which has the same ID number registered when a customer did a viewing-and-listening contract, and was forged or copied as a result was used, and the paid broadcasting system which can discover unjust viewing and listening can be realized.

[0068]According to the paid broadcasting system according to claim 2, in the paid broadcasting system according to claim 1 said customer-relations-management center, When the telephone number which is not memorized by said customer database is notified, Or since it was made to judge that the IC card to which the ID number which is not memorized by the customer database was transmitted and which was case [ the IC card ], forged or copied may have been used, In a customer-relations-management center, when the customer data which are not memorized by the customer database are received, it judges that the IC card forged or copied was used, and the paid broadcasting system which can discover unjust viewing and listening can be realized.

[0069]According to the paid broadcasting system according to claim 3, in the paid broadcasting system according to claim 1 or 2 said customer-relations-management center, Since the place of the receiver which carried out unjust viewing and listening was searched based on the telephone number to which it was notified by use of said number notice service when it was judged that said IC card forged or copied may have been used, The customer-relations-management center can trace a sending agency from the telephone number notified from the receiver which carried out unjust viewing and listening using number notice service, when unjust viewing and listening by use of the IC card forged or copied is discovered.

[0070]According to the paid broadcasting system according to claim 4, in the paid broadcasting system according to any one of claims 1 to 3, said IC card is read-only, From it being peculiar data, the ID number memorized by this IC card can specify the customer who concluded the viewing-and-listening contract of paid broadcasting data to all the customers.

[0071]In [ according to the paid broadcasting system according to claim 5 ] the paid broadcasting system according to any one of claims 1 to 4, The customer who concluded the viewing-and-listening contract of paid broadcasting data can be specified based on the serial number of the IC card which is a number peculiar to an IC card from using the serial number of said IC card as said ID number.

[0072]In the paid broadcasting system by which the customer who concluded the broadcasting station which provides paid broadcasting data, and the viewing-and-listening contract according to the paid broadcasting system according to claim 6 installs the receiver

which can receive this paid broadcasting data, and views and listens to this paid broadcasting data, The encoder which encodes paid broadcasting data, and the scrambler which carries out the scramble of said encoded paid broadcasting data with a scramble key, A scramble key generator which generates said scramble key, and an enciphering device which enciphers said scramble key with a master key, A multiplexing device which multiplexes said enciphered scramble key and said paid broadcasting data by which scramble was carried out, The broadcasting station possessing the transmission antenna which transmits said multiplexed paid broadcasting data, The receiving antenna which receives said multiplexed paid broadcasting data via a communications satellite from said broadcasting station, The tuner which performs recovery processing to said multiplexed paid broadcasting data, The descrambler demultiplexer which extracts said enciphered SUKURAMBU key and said paid broadcasting data by which scramble was carried out from said paid broadcasting data to which it restored, and performs descrambling processing to said paid broadcasting data by which scramble was carried out, The decoder which decodes said descrambled paid broadcasting data, It has said master key used for encryption processing of said scramble key at said broadcasting station, and a master key with the same information, Encryption decoding processing is performed to said enciphered scramble key which was extracted in said descrambler demultiplexer using this master key, The IC card outputted to said descrambler demultiplexer as a scramble key required for said descrambling processing, At the time of the receiver possessing a modem connectable with a dial-up line, and the viewing-and-listening contract of paid broadcasting data. The customer database which records the customer data about each customer, such as a telephone number etc. of a name, an address, the master key information memorized by the IC card, and the dial-up line connected to the receiver, and outputs said master key information to an enciphering device, The customer-relations-management center possessing the customer inquiry unit which refers for said customer data if needed, When [ in which it appears and it is constituted, and said customer views and listens to said paid broadcasting data ] it case, or views and listens, the receiver which this customer owns performs call origination via said dial-up line using number notice service to said customer-relations-management center, Transmit and the master key information memorized by said customer's IC card with the viewing-and-listening demand or the viewing-and-listening result said customer-relations-management center, The telephone number notified by use of the master key information memorized by said IC card and said number notice service, Since the telephone number of the dial-up line connected to the receiver which the master key information of said customer remembered by said customer database and said customer own was compared in said customer-data inquiry unit, The telephone number notified in the customer-relations-management center using number notice service, When the telephone numbers of the dial-up line connected to the receiver which the customer remembered by the customer database owns differ, It means that it was used at the place other than the place which the IC card which has the same master key information registered when a customer did a viewing-and-listening contract, By as a result, the thing for which the master key information which can judge that the IC card forged or copied was used, and is memorized by the IC card is used as a customer's ID number. The amount of information memorized to an IC card can be decreased, and the paid broadcasting system which can discover unjust viewing and listening can be realized more by low cost.

[0073]According to the paid broadcasting system according to claim 7, in the paid broadcasting system according to claim 6 said customer-relations-management center, When the telephone number which is not memorized by said customer database is notified, Or since it was made to judge that the IC card to which the master key information which is not memorized by the customer database was transmitted and which was case [ the IC card ], forged or copied may have been used, In a customer-relations-management center, when the

customer data which are not memorized by the customer database are received, it judges that the IC card forged or copied was used, and unjust viewing and listening can be discovered.

[0074]In the paid broadcasting system according to claim 6 or 7, the paid broadcasting system according to claim 8 said customer-relations-management center, Since the place of the receiver which carried out unjust viewing and listening was searched based on the telephone number to which it was notified by use of said number notice service when it was judged that said IC card forged or copied may have been used, The customer-relations-management center can trace a sending agency from the telephone number notified from the receiver which carried out unjust viewing and listening using number notice service, when unjust viewing and listening by use of the IC card forged or copied is discovered.

[0075]According to the paid broadcasting system according to claim 9, in the paid broadcasting system according to any one of claims 6 to 8, said master key information memorized by said IC card, It is read-only and the customer who concluded the viewing-and-listening contract of paid broadcasting data can be specified from it being peculiar data to all the customers.

[0076]In the paid broadcasting system by which the customer who concluded the broadcasting station which provides paid broadcasting data, and the viewing-and-listening contract according to the paid broadcasting system according to claim 10 installs the receiver which can receive this paid broadcasting data, and views and listens to this paid broadcasting data, The encoder which encodes paid broadcasting data, and the scrambler which carries out the scramble of said encoded paid broadcasting data with a scramble key, A scramble key generator which generates said scramble key and a work key, An enciphering device which enciphers said scramble key with said work key, and enciphers said work key with a master key further, A multiplexing device which multiplexes said enciphered scramble key, said enciphered work key, and said paid broadcasting data by which scramble was carried out, The broadcasting station possessing the transmission antenna which transmits said multiplexed paid broadcasting data, The receiving antenna which receives said multiplexed paid broadcasting data via a communications satellite from said broadcasting station, and the tuner which performs recovery processing to said multiplexed paid broadcasting data which was received with said receiving antenna, Said enciphered scramble key, said enciphered work key, and said paid broadcasting data by which Scramble was carried out are extracted from said paid broadcasting data to which it restored, The descrambler demultiplexer which performs descrambling processing to said paid broadcasting data by which scramble was carried out, The decoder which decodes said descrambled paid broadcasting data, It has said master key used for encryption of said work key at said broadcasting station, and a master key with the same information, Encryption decoding processing is performed to said enciphered work key which was extracted in said descrambler demultiplexer using this master key, Memorize the decrypted this work key and encryption decoding processing is further performed to said enciphered scramble key using this work key, The IC card outputted to said descrambler demultiplexer as a scramble key required for said descrambling processing, The master key information remembered to be a receiver possessing a modem connectable with a dial-up line by the name, the address, and the IC card at the time of the viewing-and-listening contract of paid broadcasting data, the work key information by which encryption or encryption decoding processing is carried out with this master key, The customer data about each customer, such as a telephone number etc. of the dial-up line connected to the receiver, are recorded, The customer database which outputs said master key for enciphering said work key by which it was generated with said scramble key generator to an enciphering device, The customer-relations-management center possessing the customer inquiry unit which refers for said customer data if needed, Come out, are constituted, and when [ to which said paid broadcasting data views and listens ] it case, or views and listens, said customer the receiver

which this customer owns, Call origination is performed via said dial-up line using number notice service to said customer-relations-management center, Transmit the work key information memorized by said IC card with said viewing-and-listening demand or said viewing-and-listening result to said customer-relations-management center, and said customer-relations-management center, The telephone number notified by said transmitted work key information and said number notice service, Since the telephone number of the dial-up line connected to the receiver which the work key information of said customer remembered by said customer database and said customer own was compared in said customer-data inquiry unit, The telephone number notified in the customer-relations-management center using number notice service, When the telephone numbers of the dial-up line connected to the receiver which the customer remembered by the customer database owns differ, It means that it was used at the place other than the place which the IC card which has the same work key information registered when a customer did a viewing-and-listening contract, By as a result, the thing for which the work key information which can judge that the IC card forged or copied was used, and is memorized by the IC card is used as a customer's ID number. The amount of information memorized to an IC card can be decreased, and the paid broadcasting system which can discover unjust viewing and listening can be realized more by low cost.

[0077]According to the paid broadcasting system according to claim 11, in the paid broadcasting system according to claim 10 said customer-relations-management center, When the telephone number which is not memorized by said customer database is notified, Or since it was made to judge that the IC card to which the work key information which is not memorized by the customer database was transmitted and which was case [ the IC card ], forged or copied may have been used, In a customer-relations-management center, when the customer data which are not memorized by the customer database are received, it judges that the IC card forged or copied was used, and unjust viewing and listening can be discovered.

[0078]According to the paid broadcasting system according to claim 12, in the paid broadcasting system according to claim 10 or 11 said customer-relations-management center, Since the place of the receiver which carried out unjust viewing and listening was searched based on the telephone number to which it was notified by use of said number notice service when it was judged that said IC card forged or copied may have been used, The customer-relations-management center can trace a sending agency from the telephone number notified from the receiver which carried out unjust viewing and listening using number notice service, when unjust viewing and listening by use of the IC card forged or copied is discovered.

[0079]According to the paid broadcasting system according to claim 13, in the paid broadcasting system according to any one of claims 10 to 12, said work key information memorized by said IC card can raise the security of a paid broadcasting system from the ability to update.